

UNCLASSIFIED

DEPARTMENT OF DEFENSE

DEFENSE INFORMATION SYSTEMS AGENCY

INFORMATION TECHNOLOGY EXHIBIT



FISCAL YEAR 2003 BUDGET ESTIMATE

February 2002

UNCLASSIFIED

**DISTRIBUTION STATEMENT A**  
Approved for Public Release  
Distribution Unlimited

20020314 103

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a combat support agency that performs a critical command, control, computer and intelligence systems mission in support of the President, the Secretary of Defense, the Joint Chiefs of Staff and the Joint Staff, the Combatant Commanders in Chief (CINCs), and the Department of Defense Components under all conditions of peace and war. DISA, by its charter, has a pivotal role to play in ensuring that the Department of Defense (DOD) can exploit the information technology needed to ensure the Full Spectrum Dominance described in the "Joint Vision 2010 and 2020". The operational concepts described in these documents are dependent on, and facilitated by, Information Superiority—the ability to collect and distribute to US forces throughout the battlefield an uninterrupted flow of information while denying the enemy's ability to do the same.

The primary customer, the warfighter, needs access to valid, secure, operationally relevant information in a timely manner to ensure success of military operations. The Global Information Grid (GIG) provides these advanced capabilities for warfighters worldwide. The GIG is the shared system of computers, communications, data, applications, security, people, and training and other support structures serving DOD's local and worldwide information needs. DISA's contribution to information superiority for the warfighter is to build and sustain critical components of the GIG. The core of DISA's GIG function is to promote and ensure jointness and interoperability of command, control, communications and computer systems.

DISA provides direct support to the Joint Staff and the combatant CINCs' operations. The capabilities DISA provides are driven by warfighter transmission, messaging, information security, command and control, and combat support requirements. These requirements continuously evolve with the rapid development of information technology. DISA works aggressively to achieve information technology synergy across the DOD by providing engineering, standards, architecture, modeling, simulation and assessment (MS&A), and testing support to the entire Department. DISA operational commands and field offices are forward deployed in direct support of the unified commands to ensure effective and efficient use of modern technology systems.

This submission includes estimates for implementation of cost saving initiatives included in the Strategy for Mainframe and Regional Transition (SMART) Plan. Specifically, these actions represent Phase II of that plan. SMART Phase I, which included mainframe consolidation and establishment of regional sites to support non-mainframe workloads, has been successfully completed. SMART Phase II includes the following initiatives: RSA right-sizing, overhead optimization, support services reductions and the impacts of customer initiated workload changes

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DISA's core programs are critical components of the Department's drive towards information superiority. DISA's major programs supporting this are: the **Defense Information Systems Network (DISN)**, the **Defense Message System (DMS)**, the **Global Combat Support System (GCSS)**, the **Global Command and Control System (GCCS)**, the **Common Operating Environment (COE)**, the **Defense Enterprise Computing Centers (DECCs)**, the **DOD Teleport**, the **Defense Technical Information Center (DTIC)**, the **Cyber Warning and Information Network (CWIN)** and the **Government Electronic Telecommunication System (GETS)**. The **Information System Security Program** is separated into IA Initiatives, in accordance with Defense in Depth categories. DISA also maintains a number of non-major systems.

The **Defense Information Systems Network** is the main communications network for the DOD. DISN provides the long-haul communications between CINC/Service/ Agency bases and from the bases to the deployed forces. To provide these voice, data and video telecommunications services DISN utilizes traditional landlines as well as more advanced wireless and satellite communications.

The **DOD Teleport** is the logical progression from the current Standardized Tactical Entry Point (STEP) concept, as the Teleport system will provide DOD deployed users with expanded Defense Information Systems Network (DISN) Long Haul access capacity, additional satellite communications (SATCOM) connection options (i.e. connection via more than just Defense Satellite Communications System (DSCS) X-band), and advanced SATCOM services not available at STEP or similar sites.

The **Defense Message System** is the secure writer to reader electronic mail system for the military. Based on commercial products and internationally developed standards DMS strives to provide interoperability and security for military message traffic.

The **Global Combat Support System** serves as the enabler to achieve Focused Logistics. Focused Logistics is the fusion of information, logistics, and transportation technologies to enable joint forces of the future to be more mobile, providing then a reach-back capability when deployed anywhere in the world. GCSS will provide a seamless flow of operational and sustaining base information to the warfighter, across combat support functions and between combat support and command and control functions.

The **Global Command and Control System** is the Department of Defense's system of record for Command and Control. GCCS supports the Joint Vision (JV) 2020 objectives of Dominant Maneuver, Precision Engagement, and Full Dimensional Protection. Furthermore, GCCS provides commanders with the fused near real-time view of the battlespace that aids them in the critical planning and execution of force projection.

Tying these pieces together, and allowing them to openly and seamlessly communicate back and forth is the job of the **Common Operating Environment**. COE is the architecture that provides for interoperability of all systems using the GIG. The COE is not actually a system, but a standards-based foundation for systems. Large portions of the components in the COE are commercially acquired; thus the COE includes interoperability and cost reduction as key tenets of its implementation. The COE is the DOD standard for acquisition and development of automated information systems (AIS).

The **Defense Enterprise Computing Centers** provide militarily essential computing capabilities critical to the global combat support operations of DOD. The DECCs process software applications for warfighters deployed around the world. These applications include transportation, finance, personnel, munitions, spare parts, medical supplies, and maintenance resources – all critical to military operations.

The **Defense Information Technical Center** serves as a vital link in the transfer of data among the Defense related and civilian research and development communities. DTIC provides access to and transfer of scientific, technical and management information for DOD personnel, DOD contractors and potential contractors, and other U.S. Government personnel and contractors. DTIC investigates and evaluates new technologies and applies them as appropriate to fulfill the information gathering, and dissemination requirements of supported organizations.

The **Government Emergency Telecommunication Systems** is a service which provides national security and emergency preparedness telecommunications for the President, Federal, State and local governments, and industry organizations. GETS provides users a nationwide capability for priority access to switched voice and voice-band data communications by exploiting the switching and transmission facilities of the Public Switched Network.



The **Cyber Warning Information Network**, an essential part of Homeland Defense, focuses on the rapid notification and warning to Government and private components concerning information with regard to protection of the critical national cyber infrastructure. CWIN facilitates dissemination among Federal Departments and Agencies of time-sensitive warnings regarding imminent threats or ongoing attacks against the nation's critical infrastructures.

**Information Assurance Initiatives** are stated in accordance with the Defense in Depth categories. **Defense in Depth** is the security approach whereby layers of security solutions are used to establish an adequate defensive posture through the integration of the information assurance capabilities of people, operations, and technology to achieve strong, effective, multi-layer, multi-dimensional protection. Implementation of this recognized that, due to the highly interactive nature of the various systems and networks, security solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured. A major increase in FY 2002 will improve security and improve deployment and operational agility of joint task forces and improve the situation awareness of the CINCs; improve coalition operations by deploying multi-security level devices that improve secure information sharing between the US and our coalition partners; improve the security and interoperability of DOD computer communications by defining, coordinating and managing a common DOD cyber perimeter defense policy; improve and operationalize DOD-wide end-system vulnerability management and end-system security configuration; and continue the hardening of the Defense Information Systems Network. These security issues, which DISA had formulated a plan to address, were highlighted following the terrorist attacks occurring on September 11<sup>th</sup>.

DISA's non-major programs cover all aspects of operations, from engineering to communications. Among the programs are the White House Communications Agency, Information Dissemination Management and DISA's Base Level Communications. These programs help DISA support the President, Secretary of Defense and the Warfighter.

DISA employs an integrated approach to managing its portfolio of information systems. The majority of DISA's programs are interlaced with one another, reliant on other systems for success. DMS and GCSS rely on the DISN for transport of communications and message traffic. DISN relies on the COE to ensure seamless end-to-end connectivity. Above all, each of the programs relies on Information Assurance initiatives for security.

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

**Changes from the FY2002/2003 Budget Submission**

The major changes from the Budget Submission (FY2002/2003) are the progression of the Standardized Tactical Entry Point (STEP) concept to the DOD Teleport System. Defense Information System Network deployed funds (including STEP) have been moved to the Program Element for Teleport funding beginning in FY2002. DISA has highlighted, with 300 Exhibit narratives, three additional programs – the Defense Technical Information Center, Cyber Warning Information Network and the Government Emergency Telecommunication System. DISA restated funding dedicated to Information Assurance activities in accordance with the Defense In Depth categories. The major or special interest programs indicate within the 300 Exhibit narrative the percentage of funding expended for Information Assurance activities, such as firewalls, detection of cyber attack and computer network defense. In the other programs, the increases are minor, reflecting inflation increases primarily. The following tables depict the changes in funding from the previous President's Budget to this fiscal year's President's Budget, and shows the amounts of collections and payments in the DWCF activities.

Schedule of Funding Changes  
 (\$ in Thousands)

	FY01	FY02	FY03
FY02 Amended Budget Submission	2,831,857	3,048,729	2,838,754
FY03 Budget Submission	2,785,364	3,283,480	3,844,131

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Schedule of Collections and Payments  
(\$ in Millions)

	FY01	FY02	FY03
Defense Enterprise Computing Centers			
Collections	604.5	612.8	552.1
Payments	598.5	606.8	567.0
Communications			
Collections	1889.1	1901.5	2319.9
Payments	1937.4	1889.0	2254.4

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

	FY2001	FY2002	FY2003
Development Modernization	2,785,364	3,283,480	3,884,131
Current Services	416,952	591,027	1,111,346
Major	2,368,412	2,692,453	2,772,785
Development Modernization	2,407,217	2,819,851	3,330,792
Current Services	250,671	364,993	835,230
Non-Major	2,156,546	2,454,858	2,495,562
Development Modernization	378,147	463,629	553,339
Current Services	166,281	226,034	276,116
	211,866	237,595	277,223
<u>Functional Area Applications</u>	126,542	133,334	149,548
COMMAND AND CONTROL	82,161	89,596	97,876
Major	71,754	79,366	87,710
GLOBAL COMMAND AND CONTROL SYSTEM	71,754	79,366	87,710
Development Modernization	29,404	30,471	35,423
O&M, Defense Wide	25,759	26,946	16,365
Proc, Defense Wide	3,645	3,525	3,454
RDT&E, Defense Wide	0	0	15,604
Current Services	42,350	48,895	52,287
O&M, Defense Wide	42,350	48,895	52,287

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

<b>Non-Major</b>				
<b>NUCLEAR COMMAND, CONTROL, COMMUNICATIONS (C3)</b>				
<b>SYSTEM</b>				
<i>Development Modernization</i>				
RDT&E, Defense Wide	10,407	10,230	10,166	
<i>Current Services</i>	10,407	10,230	10,166	
O&M, Defense Wide	7,223	6,988	7,269	
	7,223	6,988	7,269	
	3,184	3,242	2,897	
	3,184	3,242	2,897	
<b>INFORMATION MANAGEMENT</b>				
	44,381	43,738	51,672	
<b>Major</b>				
<b>DEFENSE TECHNICAL INFORMATION CENTER</b>				
<i>Development Modernization</i>				
RDT&E, Defense Wide	44,381	43,738	45,249	
<i>Current Services</i>	44,381	43,738	45,249	
	675	753	1,145	
	675	753	1,145	
	43,706	42,985	44,104	
	43,706	42,985	44,104	
<b>Non-Major</b>				
<b>INFORMATION DISSEMINATION MANAGEMENT</b>				
<i>Development Modernization</i>				
RDT&E, Defense Wide	0	0	6,423	
<i>Current Services</i>	0	0	6,423	
O&M, Defense Wide	0	0	6,078	
	0	0	6,078	
	0	0	345	
	0	0	345	

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

Communications and Computing Infrastructure

**USER PRODUCTIVITY TOOLS**

**Major**  
**DOD EBUSINESS PROGRAM OFFICE**

*Development Modernization*

O&M, Defense Wide

Proc, Defense Wide

RDT&E, Defense Wide

*Current Services*

O&M, Defense Wide

2,397,406	2,827,525	3,362,123
46,131	43,741	73,356
46,131	43,741	43,356
46,131	43,741	43,356
39,725	36,974	36,281
9,348	8,090	8,356
3,674	3,648	3,660
26,703	25,236	24,265
6,406	6,767	7,075
6,406	6,767	7,075

Non-Major

**CYBER WARNING INFORMATION NETWORK**

*Development Modernization*

RDT&E, Defense Wide

*Current Services*

O&M, Defense Wide

0	0	30,000
0	0	30,000
0	0	10,000
0	0	10,000
0	0	20,000
0	0	20,000

**USER PRODUCTIVITY TOOLS**

Major

**DEFENSE MESSAGE SYSTEM**

*Development Modernization*

O&M, Defense Wide

Proc, Defense Wide

RDT&E, Defense Wide

*Current Services*

DWCF Operations

86,215	91,434	96,894
86,215	91,434	96,894
36,258	38,239	39,882
10,540	8,271	8,769
14,970	18,797	19,345
10,748	11,171	11,768
49,957	53,195	57,012
49,957	53,195	57,012



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**USER PRODUCTIVITY TOOLS**

	2,458	3,898	7,794
<b>Non-Major</b>			
<b>SECURE - VIDEO TELECONFERENCING SYSTEM</b>	2,458	3,898	7,794
<i>Development Modernization</i>	0	1,397	5,300
O&M, Defense Wide	0	1,397	5,300
<i>Current Services</i>	2,458	2,501	2,494
O&M, Defense Wide	2,458	2,501	2,494

**OTHER COMMUNICATION INFRASTRUCTURE ACTIVITIES**

	39,057	145,984	113,582
--	--------	---------	---------

**Major**

**DOD TELEPORT**

*Development Modernization*

Proc, Defense Wide

RDT&E, Defense Wide

*Current Services*

O&M, Defense Wide

	39,057	145,984	113,582
	6,500	115,595	82,224
	6,500	110,887	60,220
	2,000	96,675	53,542
	4,500	14,212	6,678
	0	4,708	22,004
	0	4,708	22,004

**GLOBAL COMBAT SUPPORT SYSTEM**

*Development Modernization*

Proc, MC

RDT&E, Defense Wide

*Current Services*

O&M, Defense Wide

	32,557	30,389	31,358
	24,156	18,131	19,681
	5,100	1,830	2,442
	19,056	16,301	17,239
	8,401	12,258	11,677
	8,401	12,258	11,677

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

**OTHER COMMUNICATION INFRASTRUCTURE ACTIVITIES 1,454,255 1,739,367 2,176,659**

**Major**

**DEFENSE INFORMATION SYSTEM NETWORK**

*Development Modernization*

O&M, Defense Wide

Proc, Defense Wide

RDT&E, Defense Wide

DWCF Capital

*Current Services*

O&M, Defense Wide

RDT&E, Defense Wide

DWCF Operations

**OTHER COMMUNICATION INFRASTRUCTURE ACTIVITIES 31,031 33,740 34,538**

**Non-Major**

**BASE LEVEL**

*Development Modernization*

O&M, Defense Wide

*Current Services*

O&M, MC

**OTHER COMMUNICATION INFRASTRUCTURE ACTIVITIES 96,566 100,397 99,123**

**Major**

**COMMON OPERATING ENVIRONMENT**

*Current Services*

O&M, Defense Wide

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Non-Major				
<b>WHITE HOUSE COMMUNICATIONS AGENCY</b>				
<i>Development Modernization</i>				
O&M, Defense Wide	64,135	82,982	80,348	
Proc, Defense Wide	64,135	82,982	80,348	
<i>Current Services</i>	14,922	31,782	26,654	
O&M, Defense Wide	3,170	6,131	6,733	
	11,752	25,651	19,921	
	49,213	51,200	53,694	
	49,213	51,200	53,694	
<b>COMPUTING INFRASTRUCTURE</b>	8,700	10,158	11,610	
Non-Major				
<b>IT CORE COMPUTING</b>	8,700	10,158	11,610	
<i>Current Services</i>	8,700	10,158	11,610	
O&M, Defense Wide	8,700	10,158	11,610	
<b>INFORMATION DISTRIBUTION SERVICES</b>	610,732	640,616	659,415	
Major				
<b>DEFENSE ENTERPRISE COMPUTING CENTERS</b>	610,732	640,616	659,415	
<i>Development Modernization</i>	610,732	640,616	659,415	
DWCF Operations	23,998	79,030	51,800	
<i>Current Services</i>	23,998	79,030	51,800	
DWCF Operations	586,734	561,586	607,615	
	586,734	561,586	607,615	
<b>INFORMATION DISTRIBUTION SERVICES</b>	22,261	18,190	89,152	
Major				
<b>GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICES</b>	22,261	18,190	89,152	
<i>Current Services</i>	22,261	18,190	89,152	
O&M, Defense Wide	22,261	18,190	89,152	
	22,261	18,190	89,152	

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

<u>Related Technical Activities</u>	111,193	122,960	153,728
<b>SPECTRUM MANAGEMENT</b>	111,193	122,960	153,728
Non-Major	111,193	122,960	153,728
<b>C4I ENGINEERING</b>	17,076	14,428	13,933
<i>Development Modernization</i>	2,206	1,583	2,440
RDT&E, Defense Wide	2,206	1,583	2,440
<i>Current Services</i>	14,870	12,845	11,493
O&M, Defense Wide	14,870	12,845	11,493
<b>C4I TEST, CERTIFICATION</b>	35,672	41,389	42,429
<i>Development Modernization</i>	35,672	41,389	42,429
RDT&E, Defense Wide	35,672	41,389	42,429
<b>DARPA/DISA JOINT PROGRAM OFFICE</b>	19,136	19,314	48,129
<i>Development Modernization</i>	12,933	14,254	42,941
RDT&E, Defense Wide	12,933	14,254	42,941
<i>Current Services</i>	6,203	5,060	5,188
O&M, Defense Wide	6,203	5,060	5,188
<b>DISA CONTINUITY OF OPERATIONS &amp; TEST FACILITY</b>	15,486	21,642	22,118
<i>Development Modernization</i>	2,549	3,265	3,325
Proc, Defense Wide	2,549	3,265	3,325
<i>Current Services</i>	12,937	18,377	18,793
O&M, Defense Wide	12,937	18,377	18,793
<b>IT ENGINEERING STANDARDS</b>	23,823	26,187	27,119
<i>Current Services</i>	23,823	26,187	27,119
O&M, Defense Wide	23,823	26,187	27,119

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

Information Assurance Activities

**DEFENSE NETWORK INFRASTRUCTURE**

Non-Major				
IA DNI-ISSP				
<i>Development Modernization</i>				
O&M, Defense Wide	17,471	30,904	28,184	28,184
Proc, Defense Wide	17,471	30,904	28,184	28,184
<i>Current Services</i>	17,471	30,420	27,682	27,682
	5,802	13,157	12,954	12,954
	11,669	17,263	14,728	14,728
	0	484	502	502
O&M, Defense Wide	0	484	502	502

**DEFENSE ENCLAVE BOUNDARY**

	12,019	12,389	15,447	15,447
--	--------	--------	--------	--------

Non-Major				
IA DEB-ISSP				
<i>Development Modernization</i>				
O&M, Defense Wide	12,019	12,389	15,447	15,447
<i>Current Services</i>	12,019	12,389	15,447	15,447
	8,204	7,578	9,965	9,965
	8,204	7,578	9,965	9,965
	3,815	4,811	5,482	5,482
	2,715	4,431	4,352	4,352
	1,100	380	1,130	1,130

**DEFENSE COMPUTING ENVIRONMENT**

	11,476	13,744	15,714	15,714
--	--------	--------	--------	--------

Non-Major				
IA DCE-ISSP				
<i>Development Modernization</i>				
O&M, Defense Wide	11,476	13,744	15,714	15,714
<i>Current Services</i>	11,476	13,316	15,256	15,256
	11,476	13,316	15,256	15,256
	0	428	458	458
O&M, Defense Wide	0	428	458	458

<b>SUPPORT INFRASTRUCTURES</b>	<b>37,724</b>	<b>43,726</b>	<b>42,173</b>
Non-Major			
<b>IA SUPPORTING INFRASTRUCTURES-ISSP</b>			
<i>Development Modernization</i>			
O&M, Defense Wide	37,724	43,726	42,173
Proc, Defense Wide	37,724	43,726	42,173
RDT&E, Defense Wide	35,426	42,630	41,103
<i>Current Services</i>	14,219	20,075	17,167
O&M, Defense Wide	3,177	10,919	6,316
	18,030	11,636	17,620
	2,298	1,096	1,070
	2,298	1,096	1,070
<b>SYSTEM SECURITY METHODOLOGY</b>	<b>7,036</b>	<b>8,210</b>	<b>8,741</b>
Non-Major			
<b>IA SYSTEM SECURITY METHODOLOGY-ISSP</b>			
<i>Development Modernization</i>			
O&M, Defense Wide	7,036	8,210	8,741
Proc, Defense Wide	7,036	8,210	8,741
<i>Current Services</i>	1,663	1,573	1,556
O&M, Defense Wide	1,663	1,379	1,556
	0	194	0
	5,373	6,637	7,185
	5,373	6,637	7,185
<b>DEFENSE INFORMATION OPERATIONS</b>	<b>34,939</b>	<b>54,878</b>	<b>70,456</b>
Non-Major			
<b>IA DIO-ISSP</b>			
<i>Development Modernization</i>			
O&M, Defense Wide	34,939	54,878	70,456
Proc, Defense Wide	34,939	54,878	70,456
<i>Current Services</i>	11,985	23,864	25,951
O&M, Defense Wide	8,295	12,109	15,082
	3,690	11,755	10,869
	22,954	31,014	44,505
	22,954	31,014	44,505



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

<b>TRAINING</b>	<b>6,080</b>	<b>5,843</b>	<b>6,445</b>
Non-Major			
IA TRAINING-ISSP	6,080	5,843	6,445
Current Services	6,080	5,843	6,445
O&M, Defense Wide	6,080	5,843	6,445
<b>MANAGEMENT &amp; OPERATIONS</b>	<b>16,126</b>	<b>17,303</b>	<b>15,075</b>
Non-Major			
IA OTHER MGMT & OPERATIONS-ISSP	16,126	17,303	15,075
Development Modernization	16,126	17,303	15,075
O&M, Defense Wide	0	475	489
Current Services	0	475	489
O&M, Defense Wide	16,126	16,828	14,586
	16,126	16,828	14,586
<b>IA FOR THE TACTICAL ENVIRONMENT</b>	<b>7,352</b>	<b>12,664</b>	<b>16,497</b>
Non-Major			
IA FOR THE TACTICAL ENVIRONMENT-ISSP	7,352	12,664	16,497
Development Modernization	7,352	12,664	16,497
O&M, Defense Wide	2,618	4,727	7,445
Proc, Defense Wide	2,418	2,327	2,945
Current Services	200	2,400	4,500
O&M, Defense Wide	4,734	7,937	9,052
	4,734	7,937	9,052

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: Global Command and Control System (GCCCS)  
Budget Initiative Number: 0881  
IT Registration System Number ALDISA07 (Section 8121, FY 2000 DoD Appropriation)  
Mission Critical Status: Mission Critical

Information Technology Project or National Security System: Information Technology  
Program Activity/Mission Area: Functional Area Applications  
PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was initiated: FY 1994

Projected Date for Completion of Block IV: Early FY2004. No project end date, as GCCCS is an evolutionary program with no specific end date.

The DISA Procurement Executive reviewed and concurred with the GCCCS Annual Program Plan

Date of Last Acquisition Decision Memorandum (ADM): To date, the Milestone Decision Authority (MDA) has not issued an ADM reference GCCCS

Project is in B/C PHASE or MILESTONE, Block III Approval Dated: 6 August 2001, Phase as of current review.  
No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. Does the security of this project meet the requirements of the Government Information Security Reform Act (GISRA)? Yes ☒ No ☐
2. The funding percentage of GCCS supporting Information Assurance Activities in FY 2003: 5.4%
3. To date, the DoD CIO has not formally reviewed GCCS for CCA Compliance. The DISA CIO has formally reviewed the GCCS CCA compliance plan and has reviewed the program's ongoing activities to achieve CCA Compliance. GCCS will submit the Block IV CCA compliance during the FY03
4. GCCS does not implement electronic transactions or record keeping.
5. GCCS did not perform a privacy impact assessment on this program.

**RESOURCE REVIEW:**

1. GCCS received a budget appropriation to support FY 2002 activities.
2. During the FY 2002 Amended Budget and FY 2003 concurrent review, changes were made to the GCCS appropriation. Program changes were due to an appropriation conversion, increased O&S costs and Congressional actions.
3. Program changes were directed at the Component and Congressional levels.
4. GCCS uses a combination of analogy, actual and parametric cost methods to determine resource requirements.
5. Federal Financial Managers Improvement Act (FFMIA).
  - GCCS is not a part of the DoD Financial Management Architectural Improvement Process.
  - GCCS is not categorized as a financial management or Financial Feeder System.
  - FFMIA compliance is not applicable to GCCS.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Part I. B. Summary of Spending for Project Stages:**

<b>Component</b>	<b>Cumulative Total FY 2000 and prior</b>	<b>FY 2001</b>	<b>FY 2002</b>	<b>FY 2003</b>	<b>FY 2004 – FY 2007</b>	<b>Total</b>
<b>Planning</b>						
O&M	165.495	25.759	26.946	16.365	62.714	297.279
Procurement	26.955	3.645	3.525	3.454	14.519	52.098
RDT&E	0	0	0	15.604	70.015	85.619
Total Dev Mod	192.450	29.404	30.471	35.423	147.248	434.996
APPN or Fund 1 to n - DevMod						
<b>Total Dev Mod</b>	192.450	29.404	30.471	35.423	147.248	434.996
<b>Full Acquisition</b>						
APPN or Fund 1 to n - Dev Mod						
Totals Dev Mod						
<b>Maintenance/ Current Services</b>						
O&M	222.454	42.350	48.895	52.287	235.459	601.445
APPN or Fund 1 to n – Current Services						
Totals Current Services	222.454	42.350	48.895	52.287	235.459	601.445
<b>Totals Resources by FY</b>	414.904	71.754	79.366	87.710	382.707	1036.441

## **Part II: Justification and Other Information**

### **A. Description/Performance Characteristics:**

Global Command and Control System (GCCS) is the cornerstone of the Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior (C4I/TW) and addresses the Mission Need Statement for GCCS, 8 Jun 1995. As an initial step, GCCS replaced the Worldwide Military Command and Control System (WWMCCS) with a more capable modern system.

GCCS provides the seamless integration of Command and Control (C2) capabilities necessary to conduct joint and multinational operations into the 21st century. A key C4I capability, GCCS supports the DOD *Transformation* by focusing on *new automated data processing (ADP) concepts, injecting new technologies, incrementally fielding relevant products and participating as a member to identify revolutionary technological breakthroughs*. GCCS also supports the National Command Authorities and subordinate elements in synchronized operations from dispersed locations and provides Joint C4I to support the entire force projection cycle. GCCS provides responsive C2. It allows Commanders-in-Chiefs (CINCs) and the Joint Task Force (JTF) commanders to maintain dominant battlefield awareness through a fused, integrated, near real-time picture of the battlespace. Additionally, GCCS provides protection of friendly forces by maintaining multidimensional battlefield awareness, friendly force readiness, and defensive Information Warfare. GCCS provides a single joint C2 system for the Chairman, Joint Chiefs of Staff. As a warfighter-oriented system, GCCS provides improved information processing support in the areas of planning, mobility, and sustainment to combatant commanders, the Services, and Defense agencies as they support current and future mission to include *Noble Eagle* and *Operation Enduring Freedom*. As a system, GCCS consists of all the necessary hardware, software, procedures, standards and interfaces for worldwide connectivity at all levels of commands.

GCCS supports and manages a wide assortment of mission critical, inter-service, Service, and site-unique applications, databases and office automation tools. It provides an open system infrastructure that allows a diverse group of systems, and commercial-off-the-shelf software packages to operate at any GCCS location with a consistent look and feel. This approach allows for vertical interoperability and a shared view of the battlefield from the National Command Authorities down to the JTF component tactical commander. Similarly, GCCS also supports horizontal interoperability among the Service components and within individual Services. GCCS establishes a fused real time picture of the battlespace to the warfighter for all automated C2 operations. The GCCS implementation strategy is comprised of the following elements:

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

- a. Migrate Service's Air Tasking Order, intelligence information, readiness and training status data, logistics, and joint operations planning and execution automated C2 processes into an environment of seamless C2 capabilities. Provide increased access to shared information and improvements in the systems speed and accuracy to enhance the warfighters' capability of prioritizing and transferring data.
- b. Continue migration of warfighter information processes including meteorological and oceanographic, intelligence and imagery, enhanced message handling, and other improvements to existing capabilities. Provide expanded access and capability to CINC remote locations.
- c. Migrate Joint C2 capabilities to the Common Operating Environment (COE). COE provides common infrastructure computing services required by the migrated mission application, including database management, message handling, correlation, graphics and mapping. The projected operational and cost benefits are multifold:
  - Increased operational value by providing a more capable and robust, near real-time C2 system; increased maintainability and supportability value by using commercial-off-the-shelf hardware and software; and increased responsiveness by incremental development and shorter period between update cycles. Cost savings through streamlined acquisition techniques using commercial-off-the-shelf products, and industry/commercial standards avoiding major development; life cycle cost savings by providing open system architecture, flexible for updates, new technologies, and maintenance; and savings by migrating only Joint Staff validated C2 functionality. Increased information assurance by providing trusted computing services that have undergone extensive security testing, and by rapidly providing globally applied security patches to identified vulnerabilities.
  - Applying the COE Integration and Runtime Specification as the basis for standardization resulting in cost savings for training and new application integration.



**B. Program Management/Management Oversight:**

The GCCS program manager (PM) is COL Ronald W. Pontius and the GCCS program executive agent is the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)). The PM manages GCCS using both statutory and regulatory requirements for an acquisition category (ACAT) IAM, Major Automation Information System (MAIS) acquisition program under DoD 5000.2-R; and embraces the concept of tailoring as outlined in DoDD 5000.

The GCCS Program Manager (PM) has prime responsibility for GCCS life cycle acquisition to include program planning, execution and monitoring to ensure approved cost, schedule and functional performance goals are met. As the GCCS program executive agent, the ASD(C3I) is the GCCS Milestone Decision Authority (MDA) and as such is responsible for the review and approval of the GCCS acquisition strategy, implementation plans and program baseline goals.

The Joint Staff J3 validates, approves, and prioritizes the requirements for documentation in the GCCS Requirements Identification Document (RID). ASD(C3I) approves the acquisition strategy and each Block Implementation Plan (BIP) formerly the Evolutionary Phased Implementation Plan – EPIP). The Office of the Secretary of Defense Program Analysis and Evaluation (PA&E) does independent validation through the annual program review process.

GCCS uses the Integrated Product and Process Development (IPPD) approach as a key enabler of evolutionary acquisition and program decision support. Periodic Overarching Integrated Product Team (OIPT) and Integrating Integrated Product Team (IIPT) reviews provide the "in-process" oversight of the GCCS program.

**C. Acquisition Strategy:**

The GCCS acquisition strategy establishes the methodology for satisfying program investment and sustainment requirements. This methodology includes the use of various contract types, employs large and small contractors and is focused to achieve agency socioeconomic goals and incorporates DoD acquisition reform initiatives.

GCCS Integration and Migration efforts are primarily supported through task orders (TO) issued under competitively awarded contracts. During the next five (5) years, GCCS will endeavor to increase performance-based contracts. The Defense Information Infrastructure-Integration Contract prime contractor is Science Applications International Corporation (SAIC), McLean, VA and is supported by many subcontractors including: AB Floyd, Alexandria VA, Booz-Allen Hamilton, McLean VA, and Computer Science Corporation, Falls Church, VA.

During FY2003, GCCS will replace the expiring SAIC contract with the DISA competitively awarded Next Generation (NexGen) contract. In addition, GCCS employs Langston University, a Minority Institutions Technology Support Services (MITSS) contractor, to perform various cost based studies, i.e., economic analysis and analysis of alternative studies. During FY2002, GCCS will select a RDT&E strategic planner – the contractor will not only plan the effective use of the programs newly authorized RDT&E appropriation, but will also engage technology investment partners and conduct studies to facilitate the development and rapid transition of revolutionary technologies to warfighter capabilities.

**D. Alternative Analysis and Risk Management:**

The GCCS program was originally defined based on a "Global Command and Control (GCC) Functional Economic Analysis (FEA)" developed in 1995. The FEA documented high-level C2 goals and identified the objectives of C2 functional activities. It established functional performance measures and identified deficiencies for both the overall C2 functional area and each of the functional activities. Based on those objectives and deficiencies, it recommended various "improvement opportunities" that would be realized through the fielding of GCCS, and estimated the effects of those improvements on performance. The FEA contained an economic analysis that projected discounted savings for GCCS Increment 1 of \$442 million, with payback in FY99.

This FEA began to establish cost and performance baselines from which to assess functional area improvements in C2 for the initial increment of the program. The FEA included the life cycle costs for procurement and fielding of a modern, client/server, open-systems architecture replacement of WWMCCS; development and fielding of a COE; migration of specific C2 applications to the new architecture; and shutting down of WWMCCS.

The cost of the status quo (i.e., maintaining current operations on WWMCCS) was based on the assumption that WWMCCS hardware maintenance costs would grow at an annual rate of 11% throughout the remaining WWMCCS life cycle, consistent with actual experience on similar equipment in the Navy. Relaxing the assumption by assuming WWMCCS maintenance costs would remain constant through FY03, the present value of the savings was approximately \$100 million with payback occurring in FY01. Based on the FEA, the initial increment of the GCCS program was authorized.

GCCS recently conducted a post transformation (WWMCCS to GCCS) economic analysis (See Part III, Paragraph (B), Original Baseline). The data analyzed as part of the EA included historical data and future financial projections through FY2007. Due to the program's evolutionary development methodology, GCCS will prepare an EA to support each BIP.

**E. Enterprise Architecture and Infrastructure Standards:**

The GCCS operates as part of the new version of the COE as mandated by the "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid (GIG) Computing" and provides the information resources required by warfighters to accomplish their C2 missions.

The GCCS target architecture tailors and extends the guidance provided by the GIG architecture to meet specific C4I needs. The GCCS makes use of the services provided by the COE and extends these services into the theater/tactical level to accommodate the warrior's requirements. The GCCS makes use of the Defense Information Systems Network (DISN) for its global communications support.

Defense Information Systems Agency (DISA) is responsible for hardware and software acquisition at the National Military Command Center, the Alternate National Military Command Center, and DISA's Center for Information Technology Integration (CITI) and Joint Interoperability Test Command (JITC). All hardware and transportation requirements for these sites are included in the GCCS program budget. Additionally, existing hardware is replaced as maintenance needs dictate or through technology insertion. DISA provided funding for the purchase and installation of the initial GCCS hardware/software suites at the 37 systems of record sites (FY94/95). However, all subsequent funding of hardware/software, transportation, and installation, resulting from CINCs or Services increase in local user requirements or existing equipment exceeding its useful life are the responsibility of the sponsoring CINCs/Services/Agencies.

GCCS is developed upon the COE which forms the foundation of the GIG activities, as well as other DISA programs: DISN, Defense Message System (DMS), Global Combat Support Systems (CINC/JTF), and Component GCCS Systems.

#### **F. Security and Privacy:**

The GCCS security environment is identified in the *GCCS Security Policy* and its implementation is bound by the *Minimum Security Requirements*. The satisfaction of these requirements requires the implementation of the C2 class, Controlled Access Protection (CAP) or equivalent capabilities; GCCS runs only on SECRET Internet Protocol Network (SIPRNET - SECRET and TOP SECRET services) and is access controlled. The GCCS security environment is designed to target the C2 class level of assurance, making use of the C2 capabilities when available and cost effective. Likewise, the GCCS security environment will take advantage of products already evaluated and contained in the Evaluated or Approved Product Lists (EPLs or APLs) maintained by the National Computer Security Center (NCSC) at the National Security Agency (NSA) when available, applicable, and cost effective. Supplemental products, such as audit analysis, system configuration monitoring, etc., will be employed to aid the security staff in carrying out their duties and responsibilities.

The GCCS security configuration, although aided by automated system services and security products, is not automatic. The GCCS security environment requires the diligent and continuous employment of the safeguards and procedures identified in the policy by the GCCS security staff and users. To support this maintenance effort, the GCCS security environment requires clear and concise procedural guidelines and documents. There are two levels of documentation provided for this purpose:

- Joint Chiefs of Staff (JCS) Instructions and Manuals – These documents extend the JS policies and procedures to the GCCS site security personnel and include the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6731.01 *Security Policy* and the CJCSI 6731.01 *Security Implementation Procedures*.
- DISA Engineering Documents and Guidance – These documents describe the security implementation responsibilities and activities to the GCCS site security personnel regarding the functional application of the protection measures available

Finally, it is important to note that the goal of the GCCS system security effort and, therefore, the protective measures that comprise the security environment, is to meet or exceed the security requirements identified in the GCCS Security Policy and Minimum Security Requirements.

GCCS does not employ the use of the DoD Common Access Card – Not applicable.

**G. Government Paperwork Elimination Act (GPEA).**

The GPEA does not apply to the GCCS core mission. GCCS supports the DISA GPEA program by using online versions of standard forms. This program, however, does not include the use of on-line signatures.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

**A. Performance Based Management System (PBMS):**

The GCCS Program Manager (PM) has prime responsibility for GCCS life cycle acquisition to include program planning, execution and monitoring to ensure the meeting of approved cost, schedule and functional performance goals. The PM cost strategy is based on identifying cost to deliver capabilities that fulfill the JS-J3 prioritized requirements. This includes developing a budget through cost to benefit, trade-off and cost as an independent variable (CAIV) analysis as well as evaluating risk to cost and schedule program baselines.

GCCS maintains an OIPT with dedicated technical and functional IPT groups chartered to monitor program goal compliance throughout the GCCS life cycle. GCCS is also subject to Quarterly Budget in-progress reviews held internally within DISA.

The MDA periodically monitors achievement or deviation from goals established in the programs BIP and APB. The MDA evaluates the program's progress against the objective established in the aforementioned documents prior to authorizing progress beyond Milestones B or C. In addition, GCCS must periodically demonstrate Clinger-Cohen Compliance, conduct an EA, and monitor contractor earned value status as defined by the Federal Acquisition Regulation (FAR).



## B. Original Baseline:

The current GCCS total ownership costs (TOC) is \$1.42B (sum of the cumulative FY2000 and prior, FY2001 current estimate and FY02 to FY07 total Life Cycle Costs (LCC)).

A post transformation EA was done for the entire GCCS Program is based on program cost data. It was determined from the cost analysis that for FY02 to FY07, the total Life Cycle Costs (LCC) were estimated to be \$932M; the Program Benefits were calculated to be \$1.561M based on 23 identified program benefits and using industry standards. The Return on Investment (ROI) was calculated to be 171%, which indicates that for every dollar that is spent on GCCS, \$1.71 is returned; the payback period was calculated to be four (4) years, which indicates that over the life cycle of the GCCS program, it takes only four years for the accrued benefits to equal the investments.

- GCCS has not rebaselined since initial program establishment.
- GCCS has not experienced milestone slippages since the last president's budget.

## C. Current Baseline Information:

Cost and schedule goals	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>Previous Baseline:</b>						
Cost Goals (\$M)	418.496	74.925	81.794	82.445	366.665	1024.325
Schedule Goals (milestones)		Block III	Block IV	Block IV-V	Block V-VI	
<b>Current Estimate:</b>						
Cost Goals (\$M)	414.994	71.754	79.366	87.710	382.707	1036.531
Schedule Goals (months)		Block III	Block IV	Block IV-V	Block V-VI	
<b>Variance from Baseline Goals:</b>						
Cost Goals (\$M)	-1%	-5%	-3%	+6%	+4%	
Schedule Goals (months)		Block III	Block IV	Block IV-V	Block V-VI	

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

- Cost Goals of current approved milestone/phase: The GCCS cost goals have changed 3% (decrease) since the last President's Budget submission.  
FY 2002 Appropriated Amount     \$81.794M  
Revised FY 2002 Current Estimate     \$79.366M
- Component level and specific Congressional actions totaling \$2.4M (decrease to O&M and Procurement) were the basis of the dollar change. As of the date, GCCS has not assessed the impact of the reduced FY2002 funding.
- GCCS experienced a 3% (decreased) variance from the last submission (FY 2002 President's Budget): The variance was less than 10%.
- GCCS will identify the 3% (decreased) variance during the programs quarterly and annual performance reviews.
- GCCS does not project a 10% budgetary variance in the FYDP program.
- The FYDP cost variance is not caused by contract price/quantity changes.

**D. Actual Performance from Approved Baseline:**

Schedule Performance: During Block III, GCCS long-term goals were reached by improving interoperability and implementation of standards (e.g., communications resources, common information sources, security policies, procedures, and training). This included robust tools to allow the user to build applications in a common C2 environment.

**Performance goals:**

FY 2001 Accomplishments: Fielded GCCS Version 3.x capability; a fused-integrated command support picture of the battlespace to commanders at CINC and JTF that will provide access to combat support information from various combat support databases. Operated and maintained the current fielded system.

**FY 2002 Goals:**

- Field major GCCS capability(s) incorporating both new and enhanced GCCS infrastructure and capabilities.
  - GCCS Version 3.x and transition to Version 4.x.
- Field time sensitive patches to fielded baseline version of GCCS incorporating fixes for applicable Information Assurance Vulnerabilities (Advisories and Bulletins) published by DoD Computer Emergency Response Team (CERT).
  - Patches to GCCS Version 4.x for IAVAs and IAVBs as identified.

**FY 2003 Goals:**

- Field major GCCS releases incorporating both new and enhanced GCCS infrastructure (including Common Operating Environment (COE)) and capabilities.
  - GCCS Version 4.x
- Field time sensitive patches to fielded baseline version of GCCS incorporating fixes for applicable Information Assurance Vulnerabilities (Advisories and Bulletins) published by DoD Computer Emergency Response Team (CERT).
  - Patches to GCCS Version 4.x for IAVAs and IAVBs as identified.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**FY 2004-07 Goals:**

Support the integration of intelligence applications into GCCS, by including program management, testing, integration, GCCS Integrated, Imagery, and Intelligence problem resolution, and CINC installation support. Incorporate new mission applications, to include selected JPO ACTDs, into the system. Implement the Chairman Joint Chief of Staff's RAS. Field the RAS Output tools Air Force, Marines, and Army personnel and logistics analysis modules. RAS will replace the current readiness system, i.e., Global Status of Resources and Training, and implement the Congressional readiness guidance given in the 1999 Defense Authorization Act. Continue to add functionality throughout this period. Insert new technologies to satisfy warfighter C2 requirements to include Windows NT and Web enabled applications. Other planned accomplishments include the following: operate and maintain the current fielded system; increase the use of expert systems; collaborative planning through video teleconferencing; provide deployable systems on satellite communications for all Joint Task Forces/CINCs/Command Components; and upgrade technologies to exploit increasing bandwidth capabilities.

**E. Cost and Schedule Corrective Actions:** GCCS has not experienced significant changes to its Block IV cost or schedule profile.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

## **PART 1. A. SUMMARY OF PROJECT INFORMATION**

### **Description Information:**

Initiative Name and Acronym: Defense Technical Information Center  
Budget Initiative Number: 5024  
IT Registration System Number NA (Section 8121, FY 2000 DoD Appropriation)  
Mission Critical Status: Not Mission Critical  
Information Technology Project or National Security System: Information Technology Project  
Program Activity/Mission Area: Functional Area Applications  
PROJECT STATUS:  
Project Status: New ☐ Ongoing ☒  
Date Project was Initiated: 1945  
Projected Date for Completion of Phase; Ongoing and of Project \_\_\_\_\_.  
This project is reviewed by the Procurement Executive for DISA.  
DITC is not an acquisition project; however, procurement actions are reviewed as required.  
Date of Last Acquisition Decision Memorandum (ADM): Not Applicable  
Project is in N/A PHASE or MILESTONE, Approval Dated: \_\_\_\_\_ Phase as of current review.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DTIC is review periodically; schedule of past reviews are as follows:

- 1992 DLA Comptroller Efficiency Review
- 1998 DISA Inspector General Organizational Assessment Visit
- 1998 Comprehensive Review and Mission Rationalization Study

No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?

Yes ☒ No ☐

2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 7%

3. Has DoD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐

Per the Annual Program Plan Review held August 2001, DTIC is in compliance with the 15 performance management points applicable under the Clinger Cohen Act.

4. Does this initiative implement electronic transactions or recordkeeping? Yes ☒ No ☐

5. If Yes was this initiative included in the GPEA strategic plan? Yes ☒ No ☐

6. Was a privacy impact assessment performed on this project? Yes ☒ No ☐

**RESOURCE REVIEW:**

1. Is this project in your baseline resource?    Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
Yes. Program resources were reduced by \$142K.
3. Were changes directed at the Component level or the DoD level or due to specific Congressional actions?  
Changes were directed at the Component level.
4. How were the resource costs determined (CAIG, other costing methods, etc)?  
Resource costs were based on a percentage of Congressional reduction applied at the Component level.
5. Federal Financial Managers Improvement Act (FFMIA) is not applicable to the DTIC program, nor is this project categorized as a Financial Management of Financial Feeder System.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions				
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 – FY2007
Planning					Total
APPN or Fund I to n - DevMod		675	753	1.145	3.590
Total Dev Mod		675	753	1.145	3.590
Full Acquisition					6.163
APPN or Fund I to n - Dev Mod					6.163
Totals Dev Mod					
Maintenance/ Current Services					
APPN or Fund I to n – Current Services		43.706	42.987	44.104	188.997
Totals Current Services		43.706	42.987	44.104	319.792
Totals Resources by FY		44.381	43.740	45.249	192.587
					325.955



## **Part II: Justification and Other Information**

### **A. Description:**

DTIC was founded in 1945 to collect and disseminate scientific and technical information for DoD and its contractors and its academic partners; to sustain technological superiority; to develop and maintain the technology knowledge base; and, later, to prevent unnecessary duplication of research. In this role, DTIC serves as a vital link in transfer of data among the Defense-related government and civilian research and development communities. DTIC contributes to the management and conduct of Defense research, development, and acquisition efforts by providing access to and transfer of scientific, technical, and management information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government personnel and their contractors. DTIC also provides IT support to other functional areas within the DoD to acquire, analyze and disseminate information to support oversight and management functions and to improve overall Department of Defense management. In order to meet the requirements of these diverse organizations, DTIC investigates and evaluates new technologies and applies them as appropriate to fulfill the information gathering, analysis and dissemination requirements of supported organizations.

The exchange of information and the sharing of ideas are of vital importance throughout the Defense community. STI specifically contributes to scientific advancement and fosters American leadership in many disciplines; as such it is an integral part of research and development. Its effective management and use play a vital role in all phases of the innovation process: education, basic research, applied research and development, product development and manufacturing, and application of science and technology to meet needs in commercial, not-for-profit, and governmental markets. In its support of STI, and of other DoD information communities, DTIC carries out core knowledge management functions, such as categorizing, organizing, storing, and appropriately disseminating information for the Department. In this vein, DTIC is unique in its ability to process and control the dissemination of Unclassified, Unclassified Limited and Classified information that is the result of research performed or funded by the DoD. The particular challenge with regard to the interdisciplinary nature of research is to overcome barriers of terminology and differing methodologies and to design systems that will accommodate the needs of researchers who must go outside their principle disciplines. DTIC has implemented database and retrieval methods as well as techniques that help researchers ask the right questions to solve interdisciplinary problems.

DTIC's expertise in information technology (IT) has improved information transfer and assisted the DoD by providing continuous improvement in data storage, retrieval and assurance of integrity. Whether in the earliest processing of paper and microform documents to the latest developments in emerging IT solutions, DTIC has led the way not only in the DoD, but also among other Federal agencies. Currently, DTIC is engaged in making its combined collections more readily available to eligible users through World Wide Web

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

(Web) process development and implementation. These Web solutions are applied not only to DTIC-controlled data, but also to more than 90 sites developed and maintained on behalf of external sponsor organizations throughout the Office of Secretary of Defense, the Defense Agencies, and the Military Service secretariats and headquarters. The audiences served by DTIC through its own information resources and those it supports for other organizations include the most specific Defense communities of interest; other government agencies; academia; the media; and, in some instances, the public. DTIC's IT experience and expertise make it possible for these diverse audiences to access required information according to precise distribution mandates and individual eligibility. With all of its information products and services, DTIC's overriding goal is to provide information in a secure, scalable, stable environment, utilizing the most viable and appropriate IT solutions available.

Statement of how this project helps the agency/DoD mission; long term strategic goals and objectives (Mission goals and/or IT strategic plan).

DTIC is a focal point for the acquisition, storage, retrieval, and dissemination of Scientific and Technical Information (STI) and other types of Defense information, including data which is restricted, controlled and/or classified. DTIC serves as the front door to DoD unclassified and unlimited information resources for customers internal and external to DoD; as the door to controlled information resources for internal use; and as one-stop source for both STI and more general DoD information. Policy-makers, managers, scientist and engineers within the Department, other government agencies, academia, and the private sector look to DTIC for leadership in providing information access, sharing, and knowledge management. A key component of DTIC's information services are the Information Analysis Centers (IACs) chartered by OSD to collect, analyze, synthesize and disseminate worldwide scientific and technical information in specialized fields to support the warfighter, to prevent re-inventing research, and to promote standardization within these fields. DTIC's IAC Program Management Office provides management and oversight of 13 DTIC funded IACs which supply analytical information in highly specific technical areas to meet the strategic goals of the Office of the Director, Defense Research and Engineering as well as military operational support requirements.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DTIC implements DoD Directive 3200.12, DoD Scientific and Technical Information Program (STIP):

- DoD Instruction 3200.14, Principles and Operational Parameters of the DoD STIP;
- DoD 3200.14-M, DoD STIP Procedures Manual;
- Public Law 94-282, National Science, Engineering, and Support Technology Policy and Priorities.

DTIC is not a single project; rather, it is a multi-faceted organization that conducts many projects simultaneously. As necessary, specific tasks within DTIC have been determined to be inherently governmental. DTIC is continually analyzing its processes at all levels, and redesigning them as required to assure that organizational effectiveness remains high while cost reductions are taken wherever possible.

**B. Program Management/Management Oversight:**

Identify the process owner (business activity, military mission), executive agent, program manager, and contracting office that manages this project if not, how is this project managed?

The Defense Technical Information Center is under Business Area 4: Joint Warfighting and DoD-Wide enterprise Capabilities, and is the process owner for this program. The DTIC Administrator manages the program. The Director Defense Research and Engineering serves as the principal in OSD responsible for STI. In FY 1998, as directed by the Defense Reform Initiative, DTIC was transferred from the DDR&E to the Defense Information System Agency.

Contracting for DTIC and the Information Analysis Centers (IACs) is provided by other government contracting agencies. DTIC contracts are serviced by the Defense Logistics Agency Support Services, Corporate Contracting (DSS-OC), Columbus, OH. IAC contracts are serviced by the Defense Supply Center (DSCC), Columbus, OH.

DTIC is not a single project. Integrated Project Teams are established when necessary to complete individual projects and specific tasks initiated within the organization. The DTIC Administrator provides oversight of the progress of specific projects and tasks. DTIC's projects are also reviewed quarterly, by senior DISA managers.

**C. Acquisition Strategy:**

Contractor Support:

Contractor:	NCI Information Systems, Inc.
Address:	8260 Greensboro Drive McLean, VA 22102
Contract Type:	Onsite tech support (2 positions)/hardware maintenance
Performance Based?	No. Competed – not sole source.
Why Chosen:	Good past performance, ease of use (BPA with our contracting activity - DSS)
Contractor:	Getronics Government Solutions, LLC
Address:	7900 Westpark Drive McLean, VA 22102
Contract Type:	Onsite tech support (3 positions)
Performance Based?	No. Competed – not sole source.
Why Chosen:	Good past performance, on GSA Schedule
Contractor:	Unisys Corporation
Address:	8008 Westpark Drive McLean, VA 22102
Contract Type:	Onsite tech support (1 position), hw/sw maintenance
Performance Based?	No. Sole source
Why Chosen:	Good past performance, multi-year contract
Contractor:	Red River Computer Company
Address:	85 Mechanic Street, Suite 400 Lebanon, NH 03766-1500

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Contract Type: Unix hw/sw maintenance (Sun equipment)  
Performance Based? No. Competed - fixed price  
Why Chosen: Good past performance, on GSA Schedule

Contractor: Xerox Special Information Systems  
Address: 250 North Halstead Street  
Pasadena, CA 91107-3128

Contract Type: Xerox equipment maintenance  
Performance Based? No. Sole source - fixed price  
Why Chosen: Good past performance, on GSA Schedule

Information Analysis Centers (IACs):

Contractor: Modeling & Simulation IAC; Alexandria, VA 22311-1720  
Manufacturing Technology IAC; Chicago, IL 60616-3799  
Nondestructive Testing IAC; Austin, TX 78746  
Reliability Analysis Center; Rome, NY 13440-6916  
Survivability/Vulnerability IAC; WPAFB, OH 45433-7542  
Weapon Systems Technology IAC; Alexandria, VA 22311-1705  
Infrared IAC; Ann Arbor, MI 48118-4008  
Information Assurance Technology Analysis Center; Falls Church, VA 22042  
Human Systems IAC; WPAFB, OH 45433-7022  
Data & Analysis Center for Software; Rome, NY 13441-4909  
Chemical Propulsion Information Agency; Columbia, MD 21044-3200  
Chemical Warfare/Chemical Biological Defense IAC; APG, MD 21010-0196  
Advanced Materials & Processes Technology IAC; Rome, NY 13440-6916

The IAC contracts are all Cost Plus - Fixed Fee contracts and were chosen by competitive bid.

**D. Alternative Analysis and Risk Management:**

A cost/benefit analysis is not applicable to DTIC's overall operations; however, individual analyses have been performed as necessary for specific projects.

Analysis of alternative options. N/A

Underlying assumptions. N/A

Estimate of Risks. N/A

**E. Enterprise Architecture and Infrastructure Standards:**

This system meets the current Government wide interoperability requirements. While this requirement may not apply DTIC-wide, many of DTIC's projects have functional interoperability as an objective. A prime example is the web-based collaborative tool which DTIC has developed and implemented for the DoD Science and Technology community. This utility provides a common environment which enables users with diverse computing platforms and configurations to work together online to develop and update science and technology planning documents. This tool maximizes efficiency by eliminating repetitious file exchanges and the problem of file incompatibilities, provides greater control, and ensures document consistency. Maintenance and administration is an ongoing project.

The Automated Data Processing/Telecommunications (ADP/T) Program is primarily a central design and operations activity mission for development and support of DTIC's "unique" automated information systems (AISs) that provide for timely transfer of STI. Design, development, and maintenance of DTIC-unique AISs are accomplished principally under internal program management as well as system design and management responsibility for all of the unique AISs including the Defense RDT&E Online System (DROLS). The design of inherent security controls to protect the inadvertent compromise of classified data is of paramount importance in all AIS development activities. DTIC operates two separate Local Area Networks (LANs): the classified LAN (REDNET) which links all classified hosts and provides support for the in-house test and production classified operation and the unclassified LAN (BLKNET) which links all unclassified hosts providing the facility for unclassified end-user computing as well as Internet and Intranet access. The data processing environments are designed to function as an integral part of the functional operations of DTIC. As part of our mission to

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

support the Office of Secretary of Defense (OSD) and DoD Component Headquarters, DTIC develops and maintains approximately 100 World Wide Web sites. Concern for customer impact due to wartime demands and local support issues led DTIC to acquire commercial internet service as well as DISN connectivity. DTIC has submitted a waiver request for the commercial Internet service. These web sites, either individually or as a group, serve to present information for and about the DoD, to DoD employees, the public, the media, other U.S. Government Agencies and foreign governments. DTIC is working with OSD offices to implement the decision to move all public access web sites from OSD to DTIC within budget constraints. As the information technologies utilized to present information on the Web have become more capable and more sophisticated, DTIC has routinely adapted the most robust of these technologies to improve existing Web sites or to apply in implementing new Web publishing projects. DTIC has made it a practice to create or adopt as many automatic processes as possible.

Hardware requirements are included in this funding.

Transport (Communications and Computing) requirements are met through use of NIPRNET, SIPRNET, and Commercial Internet Service Provider (ISP)

DTIC Interfaces with the Ft. Belvoir Directorate of Information Management (DOIM) for external connectivity.

DTIC utilizes both COTS and custom components. Custom components are needed to provide for DTIC's operating environment which processes both classified and unclassified information. LANs were constructed at DTIC to bring independent classified and unclassified access to the desktop for all DTIC employees that require it. Workstations (to include classified open storage areas) have been wired and configured to support the tightly integrated operation and maximize efficiency and security. The classified LAN provides the facility for all in-house classified production processing and programming, test, and development needs. The Electronic Document Management System and document processing environments that require frequent daily movement of data among classified/unclassified systems to perform production operations are designed to perform effective workflow.

Although DTIC Web operations utilize COTS products when possible, custom applications have been developed for numerous Web sites which either pre-dated COTS application availability or have unique requirements for which there is no COTS solution. In many cases, COTS solutions that are acceptable for commercial use do not meet the strict security standards of the DISA/DTIC system environment and either must be modified with custom code or rejected for use in favor of custom-developed applications.



The existing DTIC data architecture is the cumulative product of over 40 years of software development. As such, it reflects multiple generations of database software and methodology. The data repository portion of our architecture includes flat files, multi-keyed by security classification. DTIC maintains two complete hardware infrastructures separated by an air gap to maintain total segregation of classified material from unclassified material. Databases are duplicated where needed in both environments. All major DTIC systems operate under an Authority to Operate granted by the DISA CIO and STIG compliance is maintained. The majority of legacy systems reside on Unisys Midframe computers in hierarchical databases. Other legacy systems were implemented using a 4<sup>th</sup> Generation Language that includes an internal proprietary database. Newer World Wide Web oriented client-server systems typically exist on Unix platforms using the Oracle relational database software in a server farm configuration. For some of the client-server systems, we have organized the database on network attached storage devices that support several applications. These are accessed via relational middleware such as ODBC and SQL\*NET. Our newest systems associated with our ongoing modernization efforts utilize object-oriented designs to access relational databases. In this environment, the data is accessed via middleware that is designed to hide the implementation details (schema) of the databases to provide both platform and database software independence. Some of these software facilities are being implemented as object-oriented "components" that combine data with the routines that operate on that data. This allows those components to be utilized by application software across the DTIC networks without regard to implementation details. This design is being used for a standardized internet credit card facility, a standardized document access validation facility, and other DTIC network services. Further future directions may include the greater use of using relational databases specially optimized to provide ultimate performance in ad hoc query environments for decision support applications.

The DTIC architectural framework will provide a flexible, scaleable information technology infrastructure that is suitable for applications intended for users located in individual work groups, in different organizations, or on the Internet. It will provide secure transmission capabilities that protect sensitive material from tampering or unauthorized access. It will be easily adaptable to handle large variations in accessing, processing, storage, and transmission demands.

DTIC will use cross-platform, open standards. The DTIC architecture will be a comprehensive set of protocols, standards, technologies and Application Program Interfaces for building and deploying applications for the Internet or corporate DoD intranets. The architecture will be comprised of open standards that are neutral with respect to hardware architecture, operating system and windowing system.

DTIC will use a common look and feel user interface. DTIC will use a single universal Internet client application, a single access method that can retrieve and display information and data from a myriad of different servers that may speak different protocols and deliver documents in a variety of formats. The client will simplify application development, training, and support. Applications



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

will be able to convey information in whatever form is most useful to users, including text, graphics, sound, animation, video and three-dimensional virtual worlds.

**F. Security and Privacy:**

DTIC uses the Defense in Depth Security approach.

Any records containing Privacy Act information is covered under an appropriate system of records.

Requirements for use and implementation of the DoD Common Access Card for the DTIC program have not been defined.

**G. Government Paperwork Elimination Act (GPEA)**

Initiative included in GPEA (EB/EC Strategic Plan).

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

A. Performance Based Management System (PBMS) Which Performance based management system will you use to monitor contract or project progress? Management oversight—or the system used to monitor the achievement or deviation from goals during the life cycle of the project. Earned value or alternate approach. (if not earned value what is used?)

Progress for program contracts measured by monthly status reports from contractors, briefings, and quarterly In-Process Reviews (IPRs). Planned milestone dates versus actual completion together with budgeted versus actual costs also serve as means of measurement. All invoices are certified by the COTR as being proper for payment before being forwarded to the Defense Finance and Accounting Service – Columbus. Program Plan reviews are conducted quarterly by DISA senior managers.

**B. Original Baseline :**

Provide the Analysis of Full Life-Cycle costs (estimates of total cost of ownership.) (Dollars in Millions) and performance benefits or goals for baseline segment or phase of this project. What did you expect to achieve?

The DTIC Program Element is under Budget Activity 6, RDT&E Management Support, which provides for the support of operations required for general research and development and not allocable to specific missions.

This program has been rebaselined during the budget cycles due to customer requirements, and benefits of utilizing new technology for support of operations.

DTIC has not had any milestone slippages since the last president's budget.

**C. Current Baseline Information:**

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
a. Previous Baseline:						
Cost Goals (\$M)	45.500	44.200	44.300	43.800	186.600	364.400
Schedule Goals (milestones)						
b. Current Estimate:						
Cost Goals (\$M)	45.400	44.400	43.700	45.300	192.600	371.400
Schedule Goals (months)						
c. Variance from Baseline Goals:						
Cost Goals (\$M)	100	200	600	1.500	6.000	7.000
Schedule Goals (months)						

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DTIC's budget from year to year does not exceed 10% growth.

Variances reflect reductions in personnel strength due to the Defense Reform Initiative, and an increase in FY 03 due to agency's accrual of full government share of retirement costs of current Civil Service Retirement System employees and health care costs for all future Federal retirees.

This is DTIC's first submission. There is no prior submission to compare variance.

The CIO/CFO and MDA/IPT will be informed of any variance through the Annual Performance Program Review, the Corporate Planning Report, the Annual In-Process Review, and reporting of Unfunded Investment Opportunities.

**D. Actual Performance from Approved Baseline:**

DTIC's performance goals of customer satisfaction and increase of IAC reimbursement align with DISA's performance and strategic plans in providing the best possible information technology support to the nation's warfighters, which supports the effective and efficient use of information technology in DoD by all organizations. DTIC's customer community spans every aspect of the DoD and includes operational organizations as well as direct and indirect support activities. By demonstrating steady growth in customer satisfaction, DTIC can substantiate achievement of its own goals of excellent customer service, easy information access, providing information to enhance decision-making and leveraging the technology base. IAC growth reflects the best use of information technology to analyze and communicate information of immediate use to the warfighter. This assessment will provide a formalized means for DTIC's self-examination and measurement of accomplishments as they contribute to the overall DISA and DoD goals.

DTIC core operations all contribute to the overall goal of providing information services in a way that engenders customer satisfaction. Among the specific accomplishments for this goal in FY 01 were:

- Provided substantial scientific and technological information in support of the Defense RDT&E effort by leveraging ongoing and completed research findings.
- Integrated modernization techniques and equipment to provide state-of-the-art electronic access and dissemination of DTIC products and services.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

- Enhanced efforts to convert the DTIC archive of technical reports to electronic media to preserve critical information and provide a paperless environment.
- Initiated testing of the Internet-based credit card processing system to expedite purchase of documents from DTIC.
- Promoted awareness of DTIC through outreach programs and proactive customer reaction measurement tools.

The IAC program was also prominent in DTIC's FY01 program plan and goals. IAC program accomplishments included:

- Provided core contract operations for DoD IACs to collect, analyze, synthesize and disseminate worldwide Scientific and Technical Information (STI) in support of DoD's critical technologies and the warfighter.
- Supplied substantial science and technological information in support of the Defense Technology Objectives and the Joint Warfighter Science and Technology Plan to develop and transition superior technology.
- Integrated modernization techniques and equipment to provide state-of-the-art electronic access and dissemination of IAC products and services.
- Enhanced efforts to totally convert fragile paper media historical archives into electronic media to preserve critical information and provide a totally paperless environment.
- Promoted IAC awareness through increased program development activities with particular emphasis on emerging technologies to support acquisitions, CINCs and the warfighter.
- Reviewed, revised, implemented and monitored strategic plan and performance measurements to support continual oversight, assessment, and improvement of DoD IACs.
- Provided IAC Program access to secure government networks to enable focused critical science and technology support to laboratories, acquisitions, CINCs and the warfighters.

Funding for ongoing basic operations was \$31.2M, while actual expenditure was \$31.0M. Other DTIC efforts which contribute to customer satisfaction were funded as follows: Defense Virtual Library funded at \$.4M, expended \$.4M; business process reengineering funded at \$2.4M, expended \$2.4M; architecture modernization funded at \$.4M, expenditure \$.4M. IAC funds were \$9.7M, with actual expenditure of \$9.7M

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Measurable performance benefits or goals for this segment or phase of this initiative:

FY 2001: DTIC will receive an overall customer satisfaction rating of 80% based on customer satisfaction survey responses.

FY 2002: DTIC will receive an overall customer satisfaction rating of 80% based on customer satisfaction survey responses.

Dollar value of reimbursable taskings for the DTIC sponsored IACs will increase by 8% over the previous fiscal year.

FY 2003: DTIC will receive an overall customer satisfaction rating of 83% based on customer satisfaction survey responses.

Of the total number of current FY IAC taskings, 15% will be from organizations not previously served by the IAC Program.

FY 2004-07: DTIC will receive overall customer rating of 83% based on customer satisfaction survey responses.

Dollar value of reimbursable taskings for the DTIC sponsored IACs will increase by 8% over the previous fiscal year.

Cost and Schedule Corrective actions: Variance from performance from last submission (identify which submission): Are the performance goals on track since last president's budget submission/last milestone or phase change? Identify any barriers/risks that must be accommodated. Justify variance. Describe corrective actions. Include barriers or risks to meeting schedule goals. Describe methods to reduce risk.

This is DTIC's first submission. There is no prior submission to compare variance.

## **PART 1. A. SUMMARY OF PROJECT INFORMATION**

### **Description Information:**

Initiative Name and Acronym: Joint Electronic Commerce Program Office (JECPO). DOD Directive 8190.2 policy names the JECPO in support of the JECPO. This policy has not changed, although the JECPO Director announced the name change to DEBPO in June 2001.

Budget Initiative Number: 5075

IT Registration System Number ALDISA13 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: There are three mission critical applications supported by JECPO: DOD eBusiness Exchange, Electronic Document Access and the Central Contractor Registration

Information Technology Project or National Security System: Information Technology Project

Program Activity/Mission Area: Communications and Computing Infrastructure

### **PROJECT STATUS:**

Project Status: New ☐ Ongoing ☒

Date Project was initiated: June 1998

Projected Date for Completion of Phase; \_\_\_\_\_ and of Project \_\_\_\_\_.

JECPO is reviewed by the DISA Procurement Executive.

JECPO plays an integral and vital role as part of the Defense Department's Revolution in Business Affairs, in particular, the Defense Reform Initiatives.

Date of Last Acquisition Decision Memorandum (ADM): N/A, the e-Business Program is not a designated MAIS/MDAP.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?  
Yes ☒ No ☐
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 0
3. Has DoD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐

Reviews take place through Quarterly In-Process and the Annual Program Plan (Sep), which takes place together with the POM Data calls. The DISA CIO (3) review is completed annually in Mar of each year. These reviews are to ensure continued Clinger-Cohen compliance for IT registration and certification. Next annual review is scheduled for March 2002.

4. Does this initiative implement electronic transactions or recordkeeping? Yes ☒ No ☐
5. Was this initiative included in the GPEA strategic plan? Yes ☒ No ☐
6. Was a privacy impact assessment performed on this project? Yes ☒ No ☐

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
No
3. Federal Financial Managers Improvement Act (FFMIA)
  - Is this project a part of the DoD Financial Management Architectural Improvement Process. Yes ☐ No ☒

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

- Is this project categorized a Financial management or Financial Feeder System. Yes ☐ No ☒

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions				
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2005 - FY 2007
<b>Planning</b>					
APPN or Fund I to n - DevMod					
Total Dev Mod					
<b>Full Acquisition</b>					
APPN or Fund I to n - Dev Mod	81.689	39.725	34.873	34.145	119.320
Totals Dev Mod	81.689	39.725	34.873	34.145	119.320
<b>Maintenance/ Current Services</b>					
APPN or Fund I to n - Current Services	7.600	6.406	8.868	9.211	29.845
Totals Current Services	7.600	6.406	8.868	9.211	29.845
<b>Totals Resources by FY</b>	89.289	46.131	43.741	43.356	149.165
					371.682



## **Part II: Justification and Other Information**

### **A. Description:**

System Description. DOD Directive 8190.2 states that the DOD Chief Information Officer shall establish and provide direction and oversight to the Joint Electronic Commerce Program Office (JECPO). The JECPO changed its name to the DOD eBusiness Program Office (DEBPO) in June 2001. DEBPO is the DOD Executive Agent to promote and coordinate implementation planning, implementation execution, and integration of common Electronic Business/Electronic Commerce (EB/EC) Services throughout the Department. The DEBPO, in collaboration with the DOD Components, develops and maintains an overarching Joint Electronic Commerce Program (JECP) implementation plan. The DEBPO applies, develops, implements and maintains common EB/EC capabilities to meet user requirements identified by functional users, and develops an overarching EB/EC architecture that can be integrated into EB/EC efforts throughout the Department. The DEBPO identifies and promulgates DOD EB/EC requirements to industry and standards developers; ensures consistent implementation of capabilities based on open standards for interoperability; and supports, facilitates, and accelerates the application of EB/EC common data into interoperable systems. The DEBPO oversees the development and maintenance of a secure, interoperable, cost effective, efficient, and integrated architecture and information infrastructure for the DOD, coordinating with Department components to deconflict, integrate, and coordinate information technology requirements. The DEBPO facilitates and supports the DOD Components efforts to implement EB/EC consistent with the Department's strategic goals and objectives such as: reduce costs; improve efficiency; increase effectiveness by improving the efficiency and effectiveness of process redesign; business systems modernization; strategic sourcing; infrastructure reductions; and optimal-sized inventories. DEBPO facilitates and supports the DOD Components efforts to implement EB/EC consistent with the Department's strategic goals and objectives dealing with providing a secure, flexible, reliable, affordable, integrated infrastructure to achieve high effectiveness in joint and combined operations; and to ensure that information technology is used to maximize advantage at least cost.

## **APPLICATIONS DEVELOPMENT & MODERNIZATION**

Central Contractor Registration (CCR) - The CCR is a web-based system that is the primary repository for vendor data and its use is required for vendors to conduct business with the DOD. The CCR database currently consists of procurement and financial information as well as trading partner data and it facilitates the use of electronic funds transfer for bill paying. The database allows the DOD to more efficiently comply with the Debt Collection Improvement Act of 1996; to simplify and streamline procurement by reducing duplicate requirements and processes; and to increase visibility of vendor sources for specific goods and services. Contractors are only required to register in the database one time with annual renewals. The CCR feeds into a shared data warehouse for access from a variety of financial and contract applications.

DOD Business Opportunities - The DOD Business Opportunities Model is a web-based system, which provides a single search mechanism for vendors' on-line review of DOD solicitations. Each of the Defense Services/Agencies provides links through their own web-based systems and to DOD Business Opportunities. DOD Business Opportunities will link with FedBizOpps in 2002.

Electronic Document Access (EDA) - EDA is a web-based system that provides on-line storage and retrieval of post award contracts, contract modifications, personal property and freight Government Bills of Lading (GBLs) and vouchers. Documents are stored in a compressed text format and are accessible through a web-based index, allowing the user to retrieve large volumes of information across the existing communication networks. EDA capitalizes on commercial tools that are widely used today. Benefits include the reduction of unmatched disbursements, paper consumption, and increased convenience to members of the user community.

DOD Electronic Mall (E-Mall) - The DOD E-Mall provides electronic buying capabilities. DOD E-Mall is an on-line system that can search, locate, compare, and order material based upon quality, price, and availability. It provides a single point of entry and search capability for all Internet based DOD electronic catalogs. This enables customers to buy both products and services. The DOD E-mall has a commodities corridor, an information technology corridor, and a services/construction corridor. The Services and Defense Agencies are fielding "stores" within these corridors. Users can search across and order from the following sources: DLA Inventory Control Point managed commodity items and Defense Reutilization and Marketing Office reutilization items; Defense Supply Center Philadelphia's Automated System for Cataloging and Ordering Textiles (ASCOT) electronic catalog for clothing and textiles items; Defense Logistics Agency's E-CAT electronic catalog of commercial part numbered items; Navy's Information Technology Center (ITEC) Direct electronic catalog of IT hardware and software items, Army Tactical Army Command (TACOM), and Inventory Control Point (ICP) long term contracts for photographic and lighting supplies, food services, and other mechanical items. In addition to providing one-stop visibility for ordering from all DOD electronic catalogs, the E-

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

Mall will provide one stop visibility of the status of orders. The E-Mall provides the benefits of reduced logistics response time and improved visibility of both government and commercial sources of supply, as well as facilitating the use of the Government Purchase Card.

Wide Area Workflow (WAWF) - Wide Area Workflow (WAWF) is a web-based system for electronic invoicing, receipt and acceptance. WAWF creates a virtual folder and an associated workflow that enables the vendor, the receiver, and the bill payer to work together to ensure prompt payment based on an electronically generated invoice and receiving document. Use of WAWF eliminates paper from the receipt and acceptance process in the contracting life cycle, and more importantly, mitigates penalty payments as the workflow streamlines the payment process. Capabilities will be added to address purchase request/funding document (PR/FD) and contract closeout (CC) processes. Benefits include eliminating unmatched disbursements and making all documentation required for payment easily accessible. WAWF is the system that allows DOD to reach its e-invoicing goals.

Electronic Portal Access Services (EPASS) - This JECPO prototype initiative provides a set of services for other DOD electronic business applications. The core services include Web-based user authentication, user authorization, user profile maintenance, and the capability to serve as an application's ePortal or support an existing ePortal. The EPASS project utilizes commercial off-the-shelf (COTS) software and rapid prototyping techniques. Electronic business applications initially supported by this prototype are Electronic Document Access (EDA) and Wide Area Work Flow - Receipt and Acceptance (WAWF-RA).

## ENGINEERING INFRASTRUCTURE

DOD eBusiness eXchange (DEBX) - DEBX, formerly called the Electronic Commerce Processing Node (ECPN). DEBX provides translation and transportation of transaction sets among legacy and new systems that need to interface with legacy systems, enabling interoperability among these systems. DEBX combines gateway and network entry point functions into a single environment. DEBX provides an enhanced audit trail of transactions to ensure end-to-end reliability and audibility. The role of DEBX is to serve as a single interface between the government and trading partners for conducting business. Among its customers, the DEBX supports the Defense Logistics Agency, US Transportation Command, Military Traffic Management Command, Defense Travel PMO, Defense Information Technology Agency, US Office, Wide Area Workflow, Central Contractor Registration PMO, Standard Procurement System PMO, Purchase Card PMO and the Defense Finance and Accounting Service. The DEBX customer base is growing as more and more systems owners recognize the value of:

- Rigorous end-to-end accountability within the DEBX system, with no single point of failure that could cause loss or non-delivery of data.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

- Multiple communications and encryption protocols for secure in transit delivery.
- A robust capability for translating messages between User-Defined Formats (UDF) and the American National Standards Institute (ANSI) X12 standard, which is the suite of implementation conventions used for electronic data interchange (EDA) between trading partners.
- Automated archive and retrieval mechanisms for messages and system configuration data.
- System performance information, including statistics, communications status, and system status. This includes developing interfaces with commercial systems using evolving standards.

EC Integration Services – Integration among application and infrastructure leading to a common business environment is the ultimate goal of EC. The technical infrastructure among the capabilities that will be addressed is single sign on using PKI. Shared Data is another integration option. DOD is taking major strides towards its goal of migrating paper-based military and business affairs to an electronic enterprise. Process models are being created for all business areas, and the technical architecture is continuing to evolve, addressing all business areas using the end-to-end procurement-based architecture as a model. JECPO is also developing an Electronic Portal (ePortal) capability called EPASS that will be the secure front end to all JECPO applications. The EPASS application will first be prototyped using Electronic Document Access and Wide Area Workflow, and will include:

- Data Integrity: Protect data from unauthorized modification
- Data Confidentiality: Protect data from unauthorized disclosure.
- User Identification and Authentication - Verification that entities are who they claim to be.
- Access control - Protect against unauthorized access.

**B. Program Management/Management Oversight:**

1. Organizational Information/Program Manager:

Ms. Evelyn M. DePalma  
Center for e-Business Applications  
Seven Skyline Place  
5275 Leesburg Pike

5075/Joint Electronic Program Office - IT Capital Investment Exhibit (IT - 300)

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

Falls Church, VA 22041

2. The projects that comprise the JECPO program are reviewed on an on-going basis, per individual project. Periodic reviews of all projects are conducted on a quarterly basis using the DISA review process. Twice a year, the DISA Vice Director is given a comprehensive, wall-to-wall review of the program.

**B. Acquisition Strategy:**

1. Identify major contract names; prime contractor and City, State, if awarded.

Major Contract	Prime Contractor	City	State
Central Contractor Registration	Price Waterhouse Coopers	Fairfax	VA
Product Data Markup Language	KPMG Consulting	McLean	VA
ePASS	EDS/Anvicom	Herndon/Fall Church	VA
Wide Area Workflow- Receipt & Acceptance	CACI/SSH/INRI EDS/FAIC/FISC	Chantilly/Palo Alto Reston/Herndon	VA/CA VA/VA
Performance Automated Information System	Navy/Compaq	Mechanicsburg Houston	PA TX

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

DOD EMAIL	Raytheon/Dell/ Excalibur/Red River	Falls Church Round Rock/Lebanon	VA TX/NH
Electronic Document Access	EDS/Defense Automated Printing Service	Mechanicsburg Herndon	PA VA
DOD Electronic Business Exchange	Northrop Grumman IT, Anvicom	Reston/Fall Church	VA
Electronic Commerce/Electronic Data Interchange	LMI/PCCI/Amerind	McLean	VA
Business Opportunities	Price Waterhouse Coopers	Fairfax	VA

Various types of contracting vehicles will be utilized in accomplishing the overall mission objectives. Several vendors provide analysis and development of system interoperability to legacy systems, thus eliminating the duplication of effort and functions. MITRE resources are being used to address technical architecture. Both large and small businesses have been put on contract to support applications and engineering. All of these efforts will allow the DOD to improve business efficiency by drastically reducing processing time and the amount of paper received, processed, and stored.

Identify whether the contract is performance-based and summarize the performance goals in the contract. N/A - JEPKO dollars are primarily R&D and R&D projects do not lend themselves to performance-based contracting.

#### D. Alternative Analysis and Risk Management:

Analyses of Alternatives are performed for individual JECPO projects to determine the best technical and cost effective solution. Once a selection is made, JECPO continues to survey the marketplace for additional alternatives e.g. WAWF selected a CACI solution in 1998 but has since reviewed a dozen workflow projects. EPass discovered a COTS solution in the past 3 months that will eliminate all but 10% of GOTS in the operational version.

Risk is managed through the use of Software Engineering Institute Capability Maturity Model (SEI CMM) certified organizations to develop software and extensive testing with assistance from operational risk is mitigated by a dual architecture framework in geographically disparate sites that load balance and self-COOP. Once a system is operational, failure is extremely rare.

#### **E. Enterprise Architecture and Infrastructure Standards:**

DEBPO applications meet the DOD and Agency interoperability requirements. DEBX supports interoperability among legacy systems by mapping transactions in standard EDI format.

##### **Infrastructure Strategy:**

The Electronic Business/Electronic Commerce EC/EC architecture has been completed using C4-Intelligence, Surveillance and Reconnaissance and the Technical Architecture Framework for Information Management. COTS implementation and COE compliance are utilized to ensure seamless integration in the C4-ISR architecture approach.

Hardware requirements are included in this funding.

Transport (Communications and Computing) requirements are met by the DOD Electronic Business Exchange (DEBX). The DEBX provides design, implementation and deployment of transport service capabilities. These capabilities are achieved through architectural design and infrastructure.

Interdependencies for data are handled through the DEBX maps. Integration of projects are handed through EC Integration Services.

DEBX applications are COTS-based or mixed with COTS when a COTS solution has not been available.

The Data Architecture approach consists of Standard Data (X12) Implementation Conventions (IC's) and XML.

Functional (Mission or Component) Architecture approach – JECPO and functional components must comply with DOD mandate of the C4ISR architecture approach.



#### **F. Security and Privacy:**

Security Approach (Defense in Depth) – The Information Assurance policy defines direction and guidance to the JECPO IAW DITSCAP procedures.

Privacy assessments for this initiative. N/A

Enabled for use with the DOD Common Access Card – Our design incorporates the future integration of this capability and will enable ease of integration in this area.

**G. Government Paperwork Elimination Act (GPEA)** –JECPO contributes to the GPEA initiatives by developing enterprise wide solutions for paperless contracting, paperless contract distribution and electronic invoicing e.g.

#### **PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

The mission of the JECPO is to accelerate the application of paperless electronic business practices and associated information technologies to improve DOD acquisition process, support life-cycle sustainment, and streamline other business operations. The JECPO facilitates the centralization of Electronic Commerce/Electronic Business (EB/EC) policy recommendations, planning, and coordination while maintaining decentralization of execution. It is the mission of the JECPO to match appropriate technologies with specific re-engineered business processes in a way that promotes maximum effectiveness. JECPO plays an integral and vital role in the DOD e-Business transformation.



Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

**C. Original Baseline:**

This system has not been rebaselined since initial program establishment.  
 The level of effort has not reflected a slippage since the last president's budget.

**C. Current Baseline Information:**

	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum total FY 2004 through FY 2007	Total
<b>A. Previous Baseline:</b>						
Cost Goals (\$M)	89.829	46.131	44.079	41.371	150.109	370.979
Schedule Goals (milestones)	12	12	12	12	12	108
<b>B. Current Estimate:</b>						

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

Cost Goals (\$M)	89.289	46.131	43.741	43.356	148.465	371.622
Schedule Goals (months)	12	12	12	12	48	108
<b>C. Variance from Baseline Goals:</b>						
Cost Goals (\$M)						
Schedule Goals (months)						

Cost Goals of current approved milestone/phase: Have there been changes (10% from last submission) since the last President's Budget submission? NO

What was the basis of the dollar change and how did this impact the milestone/phase/increment objectives? NO

Variance from last submission (identify which submission): If there has been a 10% change, discuss variance. NO

Describe how the CIO/CFO and MDA/IPT will be/has been informed of this variance. (Include when and by what means). N/A

If there has been a 10% change in the FYDP program, or in any fiscal year, describe and justify the variance. N/A

Cost variances are not due to contract price/quantity changes. All current changes have been mandated by ASD/C3I, who provides policy, direction and oversight.

**D. Actual Performance from Approved Baseline:** The JECPO program was established in its current form in calendar year 1997 with the first resources aligned with the new program structure for FY 1998. This Secretary of Defense introduced the concept of EB in the Defense Reform Initiative of November 1997. This report stated that "a full commitment of electronic business operations will not only result in tangible savings, but will also change the DOD's business culture, forcing managers to think differently and act more efficiently".

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

The Goal of the Center for e-Business Applications is to accelerate the application of paperless electronic business practices and associated information technologies to improve DOD business processes, support life-cycle sustainment, and streamline other business operations. This initiative provides technical, engineering and operational support to the JECPO.

FY02: Enhance functionality in DEBX to accommodate ever-increasing customer base, e.g., the Standard Procurement System interfaces with DOD legacy systems and the interface between the Defense Travel System pilot sites and their accounting systems through the 4<sup>th</sup> qtr. Continue to improve system security by adding new encryption protocols for secure in transit delivery, e.g., Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS), Pretty Good Privacy (PGP), Secure Shell/Secure Copy (SSH/SCP).

Provide required functionality in the paperless contracting product suite, specifically Wide Area Workflow, to meet DODs electronic invoicing mandate by Oct 02.

FY03: Modernize Central Contractor Registration (CCR) to a directory based service for ubiquitous access across the department as Part of the Global Directory System by Oct 03.

Expand DEBX map development and support for interfacing customers: DFAS, DTS, SPS, USTRANSCOM, DITCO, CCR, WAWF, as well as implementation of the DEBX Data Mart.

FY04-07: At a minimum, extend prototype capability to remaining major DOD functions, to include finance, transportation, medical, and logistics.

Enhance the infrastructure and provide state-of-art technology for expanding and supporting Electronic Commerce and related technologies to allow DOD to improve business efficiency and enhance security services. Overall, will provide a more responsive integrated contracting process capability.

FY 2001:   \$ 46.8  
FY 2002:   \$ 43.7

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Joint Electronic Commerce Program Office (JECPO)

FY 2003: \$ 43.4  
FY 2004-07: \$148.5

**Cost and Schedule Corrective actions:**

**Corrective Actions -**

- Changes have not exceeded 10% in the FYDP
- Cost variances are not due to contract price/quantity changes. All current changes have been mandated by ASD/C3I.
- The single most critical factor that could impact costs is the necessity to modify existing or developing contracts to meet changes in technology or methodology to mitigate new and emerging threats DII assets and infrastructure.

Barriers to meeting schedule goals – None

**Methods to reduce risk**

- Ensure compliance with Clinger-Cohen Act, by continuing of annual reviews.

## **PART 1. A. SUMMARY OF PROJECT INFORMATION**

### **Description Information:**

Initiative Name and Acronym: Cyber Warning Information Network (CWIN)

Budget Initiative Number: 6526

IT Registration System Number: Not applicable since system design is still being negotiated with the White House

Mission Critical Status: Mission Critical.

Information Technology Project or National Security System: National Security System

Program Activity/Mission Area: Communications and Computing Infrastructure

### **Project Status:**

Project Status: Ongoing

Date Project was Initiated: 15 Sep 2000

Projected Date for Completion of Phase: 30 Sep 2003 Project: Continuing.

Is this project reviewed by the Procurement Executive for your Component?

The Acquisition Plan will be reviewed by our Agency Procurement Executive IAW Agency acquisition regulations.

Date of Last Acquisition Decision Memorandum (ADM): Not applicable as this initiative is not a designated Major Automated System or a Major Defense Acquisition Program.

Project Acquisition Plan will be reviewed by the White House's interagency CWIN Working Group and will be prepared in accordance with the Agency acquisition regulations to include addressing CIO issues.

**Clinger-Cohen Act Compliance/CIO Review:**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?

Yes

2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 50%

3. Has DoD or Component CIO reviewed this project for CCA Compliance?

Yes, CWIN utilizes the Defense Red Switch Network (DRSN). The DRSN has been reviewed for CCA compliance. It should be noted that the CWIN architecture is subject to change from emerging White House requirements.

4. Does this initiative implement electronic transactions or recordkeeping? No.

**Resource Review:**

The Cyber Warning Information Network is funded in the baseline NCS budget. Events of September 11 have accelerated actions to expand NCS capability to support CWIN to an integrated government/industry cyber warning operating 24X7, and to complete actions for connectivity with other government operations centers and private industry for issuing warnings and information sharing. Costs of contracts are determined through competitive contracting procedures.

Federal Financial Managers Improvement Act (FFMIA) is not applicable to CWIN. This system does not process financial information.

**Part I. B. SUMMARY OF SPENDING FOR PROJECT STAGES:**

Component	Dollars in Millions					
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	FY 2004	Cum Total FY 2005 - FY 2007
<b>Planning</b>						
APPN or Fund I to n - DevMod	0	0	0	10.000	0	0
Total Dev Mod	0	0	0	10.000	0	0
<b>Full Acquisition</b>						
APPN or Fund I to n - Dev Mod						
Totals Dev Mod						
<b>Maintenance/ Current Services</b>						
APPN or Fund I to n - Current Services	0	0	0	20.000	0	0
Totals Current Services	0	0	0	20.000	0	0
<b>Totals Resources by FY</b>	0	0	0	30.000	0	0
						30.000

## **Part II: JUSTIFICATION AND OTHER INFORMATION**

### **A. Description/Performance Characteristics:**

The focus of the CWIN is the rapid notification and warning to Government and private components concerning information with regard to protection of the critical national cyber infrastructure. As such, CWIN facilitates dissemination among Federal Departments and Agencies of time-sensitive warnings regarding imminent threats or ongoing attacks against the nation's critical infrastructures. This capability will provide a Federal coordination capability mitigate the effects of cyber attacks. CWIN utilizes the secure private government DRSN and the Alerting and Coordinating Network (ACN) for extension to industry operating centers to provide simultaneous notification/communication among infrastructure protection entities, further enabling and facilitating the capability for real-time information sharing within Government and between Government and Industry. The ACN is a highly reliable voice communication path which is independent of the public telecommunications network. It also provides 24X7 operation and watch capabilities via the NCS' National Coordinating Center for Telecommunications - Information Sharing and Analysis Center (NCCC-ISAC) to support the ability to issue alerts and warnings in near real-time. Research and development is being conducted to develop tools to monitor the health of the public network (PN) and identify cyber anomalies.

### **B. Program Management/Management Oversight:**

The CWIN is being managed by the Office of the Manager, NCS. The Secretary of Defense is the Executive for the NCS. The CWIN working group, chaired by the National Security Council, provides oversight for this project. Additionally, CWIN development is coordinated between National Cyber Threat Action Group (NCTAG) members, such as the National Security Council (NSC), Joint Task Force for Computer Network Operations (JTF-CNO), National Security Agency (NSA), National Infrastructure Protection Center (NIPC), the Federal Computer Incident Response Center (FedCIRC), and the US Secret Service (USSS).



**C. Acquisition Strategy:**

ARTEL, Inc., Reston, VA, was chosen to perform initial site surveys, architectural support and technical assistance for early implementation of CWIN. Arrowhead Space and Telecommunications, Inc., Falls Church, VA, was chosen to maintain and expand the Alert and Coordinating Network (ACN) in support of the CWIN initiative to provide simultaneous notification/communication among infrastructure protection entities. The DISA IAssure contract at Scott AFB in Illinois is used to support the provision of a 24X7 operations and watch capabilities on behalf of the NCC-ISAC, further enabling the capability for real time information sharing. Akamai, Cambridge, MA, AT&T, Basking Ridge, NJ, the Department of Energy's National Laboratory in Sandia, NM, and Booz-Allen & Hamilton, McLean, VA, are being considered to conduct research and development for the expansion of CWIN specifically to develop a communications architecture designed to facilitate the immediate sharing of critical cyber information within Government, and ultimately, with industry.

**D. Alternative Analysis and Risk Management:**

As a result of 9/11, the OMNCS accommodated the White House tasking for accelerated implementation of CWIN. CWIN initially utilizes and expands the existing DRSN to support the mandate for a communications architecture to facilitate the immediate sharing of critical cyber information within Government, and ultimately, with industry. Utilizing and leveraging the existing DRSN network architecture and assets proved to be an economical and cost effective means for accelerated fielding of CWIN. CWIN will utilize the Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS) for classified collaboration and communications. The Interagency Cyber Warning Information Network Subgroup provided the initial assessment for a cyber warning network, with subsequent assessments being conducted in a collaborative high-level joint interagency environment.

**E. Enterprise Architecture and Infrastructure Standards:**

CWIN utilizes DSRN's previously approved network architecture, thus complying with limited access infrastructure requirements.

**F. Security and Privacy:**

This is a secure network. POC is Don Smith, NCS Program Manager. He can be reached at (703)-607-4910.

**G. Government Paperwork Elimination Act (GPEA):**

CWIN is utilizing the DRSN to provide expeditious sharing of information of actionable alerts and notifications among member Government organizations, and ultimately with industry. The network serves the purpose for early alerts and warning and it not being used for data storage and record keeping so GPEA is not applicable.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

**A. Management System:**

The OMNCS employs management oversight to monitor adherence to predetermined cost, schedule, and performance targets. Specifically, quarterly reviews will be conducted to compare baseline targets to actual achievements to ensure target goals are met. Close coordination and collaboration, and oversight occurs with the interagency National Cyber Threat Action Group (NCTAG), chaired by the NSC.

**B. Original Baseline :**

In January 2000, the National Coordinator for Security, Infrastructure Protection, and Counterterrorism designated the National Communications System (NCS) National Coordinating Center (NCC) as the Information Sharing and Analysis Center (ISAC) for telecommunications. The initial NCC-ISAC membership was based on NCC membership, which is evolving to reflect a broader base of technologies comprising the telecommunications infrastructure. NCC-ISAC supports the mission assigned by Executive Order 12472 and the national critical infrastructure protection goals of government and industry. The NCC-ISAC provides the means for collaboration and information sharing among its participants gathering from and disseminating to telecommunications industry and Government participants information on vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, government, and other sources.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: National Communications System

Additionally, the NCC-ISAC analyzes cyber anomaly data with the goal of averting or mitigating impact upon the telecommunications infrastructure.

**C. Current Baseline Information: \***

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)	0	0	0	0	0	0
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)	0	0	0	30.000	0	30.000
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)	0	0	0	30.000	0	30.000
Schedule Goals (months)						

**Cost Goals:.**

As a result of the September 11 events, the NCS budget for CWIN has been increased by \$30 million in FY2003. The goals to be reached include an architecture development, operations support and information dissemination. A Communications architecture will be developed that is designed to facilitate the immediate sharing of critical cyber information within government, and ultimately with industry. The OMNCS will ensure that all CWIN-related operations are properly supported during all crises and emergency situations. Finally, critical cyber information will be shared with government agencies as well as essential NCS industry partners. CWIN goals have been accelerated in response to White House taskings related to 11 Sep 2001 events.

**D. Actual Performance from Approved Baseline:**

Timely implementation of CWIN is essential to critical infrastructure protection (CIP). Specifically, CWIN will provide timely alerts and notifications as indicators point to attacks on the Nation's critical infrastructures, especially the telecommunications backbone in the PN. As has been documented in National policy documents, the PN provides essential services, which much of the Nation's economy and services are dependent upon. Because timely implementation is essential, metrics center around meeting the baseline implementation schedule.

**Describe the measurable performance benefits or goals for this segment or phase of this initiative.**

- FY 2001: CWIN IOC was achieved within schedule for the seven designated Government sites on the inner ring
- FY 2002: Enhanced CWIN capabilities will be achieved within schedule for the seven designated Government sites on the inner ring along with an initial outer ring architecture to accommodate CWIN expansion to other Government sites and to industry.
- FY 2003: Complete CWIN outer ring architecture
- FY 2004-07: Continue to implement CWIN expansion with industry.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: Defense Message System (DMS)

Budget Initiative Number: 0615

IT Registration System Number ALDISA02 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: Mission Critical System

Information Technology Project or National Security System: Information Technology Project  
Program Activity/Mission Area: Defense Message System (DMS)

### PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was Initiated: 1988

Projected Date for Completion of Phase: Ongoing and of Project: Ongoing.

This project is reviewed by the Procurement Executive for DISA DoD-wide acquisition program oversight provided by ASD (C3I) as part of ACAT 1A review process.

Date of Last Acquisition Decision Memorandum (ADM): 27 April 2001

Project is in Fielding/Deployment PHASE or MILESTONE, Approval Dated: \_\_\_\_\_ Phase as of current review.

While the ADM dated 27 April 2001 does not specifically say Phase or Milestone number, it allows for "immediate deployment: to meet operational needs. Milestone C is scheduled for 3<sup>rd</sup> Quarter FY 2002.

No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?  
Yes ☒ No ☐
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: DMS IA support is included in the Information Systems Security Program resources of DISA. The percentage of IA support in the DMS Initiative is approximately 33%.
3. Has DoD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐  
Documents are being prepared and staffed for review by 3<sup>rd</sup> Quarter of FY02. DMS CCA compliance reviews are conducted in DISA's Annual Program Spend Plan Review process, as well as the MAIS IPT/OIPT review process which entails Clinger-Cohen areas specified in DOD 5000.2-R.
4. Does this initiative implement electronic transactions or recordkeeping?  
  - If Yes, was this initiative included in the GPEA strategic plan? Yes ☒ No ☐
  - If No, discuss in Part 2, Section G? Yes ☒ No ☐
  - Was a privacy impact assessment performed on this project? Yes ☒ No ☐

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
No.
3. Were changes directed at the Component level or the DoD level or due to specific Congressional actions? No
4. How were the resource costs determined (CAIG, other costing methods, etc)? Joint Economic Analysis
5. Federal Financial Managers Improvement Act (FFMIA)
  - Is this project a part of the DoD Financial Management Architectural Improvement Process. Yes ☐ No ☒
  - Is this project categorized a Financial management or Financial Feeder System. Yes ☐ No ☒

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions					
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	FY 2003	Cum Total FY 2004 - FY 2007
<b>Planning</b>						
APPN or Fund 1 to n - DevMod						
Total Dev Mod						
<b>Full Acquisition</b>						
APPN or Fund 1 to n - Dev Mod	371.843	36.258	38.498	40.221		165.012
Totals Dev Mod	371.843	36.258				651.608
<b>Maintenance/ Current Services</b>						
APPN or Fund 1 to n - Current Services	97.724	49.954	53.195	58.988		208.727
Totals Current Services	97.724	49.954				466.612
<b>Totals Resources by FY</b>	469.567	86.212	91.693	97.009		373.739
						1118.220

## Part II: Justification and Other Information

### A. Description:

1. The Defense Message System (DMS) addresses the evolutionary Department of Defense (DoD)-wide transition from the Automatic Digital Network (AUTODIN)/E-mail baseline to the target architecture for organizational and individual messaging, maximizing the use of commercial off-the-shelf software components based on international standard protocols. The DMS messaging and directory services will replace AUTODIN and legacy mail systems for organizational messaging and individual mail, utilizing the Defense Information Systems Network (DISN). National Security Agency's (NSA) Multilevel Information Systems Security Initiative(MISSI) products will provide security protection. The DMS Multi-command Required Operational Capability (MROC) 3-88, change 2, 30 October 1997 Joint Staff (J6) memorandum, defines the primary DMS objective as reducing costs and staffing requirements for DoD messaging services. Secondary objectives are to improve messaging security and service.
2. This project supports the Defense Information Systems Agency (DISA) strategic goal of providing easy sharing of high quality information to support interoperability among U.S. forces and allies while providing command and control/secure messaging capability for the Warfighter.
3. The pre Milestone 0/ Planning activities that lead up to this decision, Business Process Reengineering, Migration plan; other approaches are:
  - OASD (C3I) memorandum, Program Guidance on the Defense Message System, Aug 88;
  - Multi-command Required Operational Capability (MROC)(3-88), The Defense Message System (DMS), Feb 89; DMS Target Architecture and Implementation Strategy (TAIS), Dec 88; DMS Working Group, DMS Panel, and DMS Implementation Group chartered by OASD(C3I)
4. The September 1993 DMS Business Plan compared three alternative strategies for migration from AUTODIN and legacy e-mail systems to Defense Message System objectives; the current strategy is the one which was shown to be the most cost effective while meeting validated requirements. The May 1998 DMS Benefits Analysis documents a Life-Cycle Cost (LCC) savings of \$668M (FY97 dollars), and a Return on Investment (ROI) of 1.45.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

#### **B. Program Management/Management Oversight:**

The process owner is the Joint Staff/J6; Program Manager is DMS PMO, DISA; Contracting office is Air Force Standard Systems Group (SSG/PKT), Gunter Annex, Maxwell AFB, AL.

In accordance with DODD 5000.1 and DODR 5000.2-R, this project is supported by Information Technology (IT) Overarching Integrated Product Team (OIPT), with working level IPTs for Cost and for Testing.

#### **C. Acquisition Strategy:**

Major contract names; prime contractor and City, State, if awarded are:

- DMS Contract, Lockheed Martin Corporation (LMC), Manassas, VA provides for the design, development, deployment, implementation and maintenance of DMS.
- Various support contractors to include: Booz Allen Hamilton for implementation, tactical deployment, configuration management and logistics support; PRC/SRA for the development and integration of Medium Grade Service (MGS); Getronics for site implementation support and site technical assistance; Data Systems Analyst (DSA) for system and software engineering support, i.e., implementation engineering, tactical integration, service management system integration support and Top Secret Collateral support; SETA Corp., for program management support, i.e., IT OIPT Team, DMS IPT, DMS Information Management support, and maintenance and evolution of DMS life cycle cost estimate; MITRE Corp., for engineering and interoperability support.
- Security products are acquired from the National Security Agency (NSA).

The contract with Lockheed Martin Corporation(LMC) was awarded under a source selection through competition. It was awarded with Cost Plus Fixed Fee, Firm Fixed Price and Fixed Price Labor contract line items for the duration of the contract. The Government chose this contract type due to the type of support the contract provides to the Government. For example, the Cost Plus Fixed Fee was chosen as the best type to provide performance incentives for overall management of contract work efforts.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

LMC is assessed quarterly against criteria contained in the contract Award Fee plan. The contractor is rated against the following criteria used in the award fee plan: Technical Performance, Business Management, and the ability to control costs, schedule and service.

**D. Alternative Analysis and Risk Management: Describe AoA.**

Cost/benefit analysis: "The DMS Revision for Flexible Architecture – A Benefits Analysis" of May 1998 finds "...substantial cost savings attributed to the shutdown of the costly and manpower-intensive AUTODIN organizational messaging system and significant user productivity savings in labor effort and reductions in cycle time which result from the improved DMS messaging process. Organizational messaging will cost less, information will be received much quicker, and messages will require much less effort to process." The Benefits Analysis applied the DISA Comptroller Economic Analysis Model and shows the net present value of DMS cost savings over the FY 1998 – FY 2010 timeframe is \$457 million. The Benefits/Investment Ratio is 1.45.

Analysis of alternative options: The September 1993 DMS Business Plan compared three alternative strategies for migration from AUTODIN and legacy e-mail systems to DMS objectives. The current strategy is the one shown to be the most cost effective while meeting validated requirements.

Underlying assumptions:

- Provides capabilities essential for AUTODIN closure
- Based on DMS Flexible Architecture
- 373K users at 250 sites (Local Control Centers)
- Costs include Unclassified and Secret Organizational users only
- Does not include TS/Collateral or deployed users

Estimate of Risks: Source: DMS Cost Analysis Description (CARD), May 1998

**E. Enterprise Architecture and Infrastructure Standards:**

This system meets current Government wide, DoD and Agency Interoperability requirements. DMS meets Joint Staff specified interoperability requirements. DMS has been independently tested for compliance with each software upgrade.

Infrastructure Strategy: DMS Infrastructure hardware requirements are included in this funding. Hardware for Service & Agency users is acquired with Service/Agency funds. Reference: Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I) memo, Defense Message System (DMS) Policy Guidance Update, 19 Feb 98.

Backbone infrastructure hardware requirements are included. Hardware for full fielding are responsibility of Services and Agencies.

The transport communications requirements are met by a combination of the DISN Wide Area Network (WAN) and the base-level Local Area Networks (LANs). Computing requirements are met by a combination of dedicated DMS hardware for the infrastructure components and shared hardware for functions such as DMS end-user components (e.g., DMS clients).

DMS relies upon the availability of local bandwidth as supplied by base-level LAN infrastructures, and upon the availability of bandwidth between the local LANs and the DISN infrastructure. These requirements are generally in line with the bandwidth requirements for commercial e-mail systems and are met by the normal communications provisioning practices of the services/agencies.

DMS consists of a integration of COTS products with a relatively small percentage of add-on software developed specifically for the DMS. The use of this custom software is required as there is no purely COTS software meeting the validated military unique requirements (e.g., military priority/precedence, automated access controls on a per-message basis supporting classifications/compartments/categories, etc.) which are defined by the DMS Multi-Command Required Operational Capabilities (MROC).

DMS is an enterprise-level electronic messaging system.

DMS is an application system that relies on the Defense Information Systems Network (DISN) for transport layer services. The DMS will be deployed essentially as four separate security domains: Unclassified, Secret, Top Secret Collateral (TS/C) and Sensitive Compartmented Information (SCI). At the Unclassified level, network connectivity between users/enclaves is generally via the Non-classified Internet Protocol Router network (NIPRNET). At the Secret level, network connectivity is generally via the Secret Internet Protocol Router

Network (SIPRNET). High Assurance Guards (HAGs) will be used to pass traffic between the security domains (i.e. Secret to Unclassified). TS Collateral traffic will transit the SIPRNET as a tunneled "virtual" network through the use of In-line Network Encryptors (INEs). DMS-based TS/C connectivity will be largely dial-up due to the small volume of traffic requirement. The Intelligence Community (IC) has four primary SCI networks supporting four Intelligence Community Infrastructure Providers (ICIPs). The IC DMS bridge points between the ICIPs are called border sites. Although the ultimate goal is to interconnect the TS/SCI and Secret collateral networks via HAGs, the near-term DMS architecture retains cryptographically separate domains primarily because of security and accreditation concerns. The Allied, tactical, intelligence, and non-DOD users each have their mission-unique messaging systems, requirements, and interfaces. The Multi-Function Interpreter (MFI) provides translation services between DMS and legacy message format users; and DMS Transition Hubs (DTHs) are the primary means of providing interoperability between DMS and legacy messaging systems. The IC is transitioning off AUTODIN via their "AUTODIN bypass" system that will interconnect existing IC switched and message processing equipment such as the Defense Intelligence Agency's (DIA) Communications Support Processor and NSA's Newsdealer using IC data networks. AUTODIN bypass will remain in effect until DMS provides sufficient capability for the IC to transition organizational messaging from their legacy systems to DMS.

#### **F. Security and Privacy:**

The DMS implements Defense in Depth by reliance upon a full range of security mechanisms to protect DMS message, directory, and management information as well as to protect the DMS messaging system itself. The DMS messaging products use the NSA developed Fortezza card, in conjunction with a special suite of security protocols, certificates and algorithms, to protect the integrity and confidentiality of DMS high grade messages. Medium grade service makes use of commercial security mechanisms, in conjunction with DoD PKI certificates, to protect the integrity and confidentiality of individual mail. The protection of the directory system, in particular the master directories and the sources of directory updates, is supported by implementation of a Virtual Private Network (VPN) between DMS components and the management centers. As DMS rides on the communications infrastructure provided by DISN and base-level LANs, firewall protections and intrusion detection mechanisms are implemented at appropriate locations within this communications infrastructure to protect the DMS components and system. NSA developed High Assurance Guards are used to protect the interconnections between different security domains (e.g., between Unclassified and Secret domains). The DMS applications execute on commercial hardware platforms with commercial operating systems. These operating systems are configured in compliance with the applicable

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

Security Technical Implementation Guidance (STIGs), further protecting the DMS components and system. This range of security mechanisms (Defense in Depth) is what provides the high degree of protection for the DMS.

DMS does not permit public access. DoD Class 3 and 4 Public Key Infrastructure (PKI) certificates are used for authentication and access control. The system does not use or contain personal information.

DMS utilizes the DoD Common Access Card for high grade (organizational/military grade) messaging the DMS makes use of the Fortezza card, which supports message signature and encryption using NSA approved algorithms and protocols and supports the requisite level of protection for DMS unclassified and classified messaging. At this time, the Common Access Card (CAC) does not provide the requisite level of support to meet the requirements of the DMS high grade messaging. The CAC does support the requirements for medium grade (individual) mail, and work is on-going to ensure that the DMS products fully support the use of CAC for medium grade service. This is targeted to be fully supported in 2003.

**G. Government Paperwork Elimination Act (GPEA):**

DMS facilitates achievement of the overarching strategic objectives for Electronic Commerce in DoD, as outlined in the DoD Implementation Plan for the GPEA (EB/EC Strategic Plan dated May 1999, Section B1.5.2.3) DMS also provides state-of-the-art security for messaging at all classification levels, per the security architecture objectives of the EB/EC Strategic Plan (Section B.2.4.6.2).

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

A. Performance Based Management System (PBMS) Which Performance based management system will you use to monitor contract or project progress? Management oversight – via ASD (C3I) Milestone Reviews.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

**B. Original Baseline:**

The DMS program is currently working to complete a new Economic Analysis (EA) which will include a Life Cycle Cost Estimate and Benefits Analysis. ASD (C3I) has established an Integrating Integrated Product Team (IIPT) and a Cost Working-level IPT (WIPT) to oversee and coordinate all efforts related to completing the EA. The Cost WIPT plans to complete the new EA by 3<sup>rd</sup> Quarter FY 2002. Information included in this section is based on the 1998 DMS EA.

- Has this system been rebaselined since initial program establishment. If so, when and why. Yes. The last MROC change.
- Has this system had milestone slippages since the last president's budget? Yes

**C. Current Baseline Information:**

1. What are the cost and schedule goals?		Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>							
Cost Goals (\$M)		469.567	87.900	92.517	97.137	375.378	1122.499
Schedule Goals (milestones)							
<b>b. Current Estimate:</b>							
Cost Goals (\$M)		469.567	86.215	91.693	97.009	384.513	1128.997
Schedule Goals (months)							
<b>c. Variance from Baseline Goals:</b>							
Cost Goals (\$M)		0.00	-1.685	-0.824	-0.128	9.135	6.498
Schedule Goals (months)							

- Cost Goals of current approved milestone/phase: Have there been changes (10% from last submission) since the last President's Budget submission? No.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

- What was the basis of the dollar change and how did this impact the milestone/phase/increment objectives? N/A
- Variance from last submission (identify which submission): If there has been a 10% change, discuss variance. There was not a 10% change in the FYDP program.
- Describe how the CIO/CFO and MDA/IPT will be/has been informed of this variance. (Include when and by what means).

Quarterly Defense Acquisition Executive Summary (DAES) Reporting and IT OITP reviews.

- If there has been a 10% change in the FYDP program, or in any fiscal year, describe and justify the variance. There was not a 10% change in the FYDP program.
- If the cost variance is caused by contract price/quantity changes, describe. N/A

**D. Actual Performance from Approved Baseline:**

DMS does not have an approved baseline (submitted on 10 September 1999 and currently still in review/coordination with OSD). New APB under development.

The DMS Program performance measures generally fall into the Strategic/Agency Level and Operational Level categories. In addition, all DMS Program performance measures support the delivery of products and services which are, in turn, designed to meet the validated requirements of the DMS Multicommand Required Operational Capability (MROC), Change, 2, 30 October 1997 (reviewed/revalidated, August 2001). The DMS MROC serves as the requirements basis for all DMS projects and component. Below is a list of the DMS MROC requirements.

1. Connectivity/Interoperability
2. Guaranteed Delivery/Accountability
3. Timely Delivery
4. Confidentiality/Security



Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: DEFENSE MESSAGE SYSTEM

5. Sender Authentication
6. Integrity
7. Survivability
8. Availability/Reliability
9. Ease of Use
10. Identification of Recipients
11. Message Preparation Support
12. Storage and Retrieval Support
13. Distribution Determination and Delivery

Measurable performance benefits or goals for this segment or phase of this initiative are:

**FY 2001:**

- Fielded Release 2.2
- Enhanced and Test Release 3.0
- Completed TS/C Infrastructure Implementation
- Completed transition of DoD GENSER Unclass, Secret, & TS/C Organizational Users to DMS
- Began Transition of Non-DoD Agencies to DMS
- Continue Deployed Tactical implementation
- Expanded/Formalized Medium Grade Service (MGS)/Begin MGS High Grade Integration/Migration
- MGS Rollout/Implementation Support to USEUCOM/USCENTCOM/STRATCOM
- Began Intel Community Implementation
- Completed Directories Upgrade
- Began Management Workstation Upgrades which provides an integrated tool for DMS service management
- Upgraded MTA/MFI Infrastructure Platforms
- COTS & PKI Evolution Support rendered.
- Hosted two DMS conferences, which provide information on the DMS transition and provide opportunities to actively participate in the sessions and one-on-one interaction with the DMS team leads, product vendors and other Users and System Administrators regarding the benefits of using DMS.
- Planned/conducted ST&Es – what are these?



Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: DEFENSE MESSAGE SYSTEM

- Implemented Second Joint Communications Support Element (JCSE) DMS Suite to support DMS Deployed users
- Participated in JWID & DMS exercises
- Implemented & Maintained Automated Message Handling System (AMHS) at CINC locations to support operational migration to DMS
- Began Virtual Private Network (VPN) Installation
- Purchased & Implemented CAW 4.2.1
- Revised Messaging Concept of Operations for MGS/Release 2.2/Release 3.0/Lessons Learned
- Sustained & operate
- Gathered & incorporate Lessons Learned

**FY 2002:**

- Successful Release 3.0 Operational Test
- Field Release 3.0
- Sustain Automated Message Handling System (AMHS) at CINC locations
- Complete VPN Installation
- Prepare for AUTODIN Closure Operational Test Fall/Winter CY02
- Deliver Release 3.0/MR1 to JITC
- Complete Upgrade of Management Workstations
- Participate in JWID, JUICE and other DMS tactical exercises
- Continue Deployed Tactical Implementation
- Expand Medium Grade Service Implementation
- Continue INTEL Community Implementation
- Continue Transition of Non-DOD Agencies to DMS
- Develop Allied Gateways Solution
- Continue COTS and PKI Evolution
- Begin Development of Release 3.1
- Conduct Release 4.0 Prototypes
- Sustain and Operate the system

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

**FY 2003:**

- Complete Release 3.0/MR1 Operational Assessment/Test
- Field Release 3.0/MR1
- Deliver Release 3.1 to JITC
- Field Allied Gateways Solution
- Complete Intel and Deployed Tactical Implementation
- Complete transition of Non-DoD Agencies to DMS
- Expand Medium Grade Service (MGS)
- Begin Development of Release 3.2
- Continue COTS and PKI Evolution
- Support Closure of DTHs
- Sustain and Operate
- Gather and Incorporate Lessons Learned

**FY 2004-07:**

- Complete Release 3.1 Operational Assessment/Test
- Field Release 3.1
- Deliver Release 3.2 to JITC
- Stabilize INTEL and Deployed Tactical Implementation
- Stabilize transition of Non-DoD Agencies to DMS
- Expand Medium Grade Service (MGS)
- Begin Development of Release 4.0
- Continue COTS and PKI Evolution
- Close Legacy Components of DTHs
- Sustain and Operate
- Gather and Incorporate Lessons Learned

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: DEFENSE MESSAGE SYSTEM

Cost and Schedule Corrective actions: Variance from performance from last submission (identify which submission): Are the performance goals on track since last president's budget submission/last milestone or phase change? Identify any barriers/risks that must be accommodated. Justify variance. Describe corrective actions. Include barriers or risks to meeting schedule goals. Describe methods to reduce risk.

There was not a 10% variance from FY 2003 Budget Estimate Submission.

1. Identify and discuss corrective actions that have been or will be taken if the current cost or schedule estimates have a negative variance.  
N/A
2. Identify the effect the actions will have on cost, schedule and performance. N/A
3. Include barriers or risks to meeting funding/cost goals. Describe methods to reduce risk. N/A

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: DoD Teleport.

Budget Initiative Number: 6462

IT Registration System Number ALDISA11 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: Mission Critical

Information Technology Project or National Security System: National Security System (NSS)  
Program Activity/Mission Area: Communications & Computing Infrastructure (C&CI)

### PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was Initiated: 20 Sep 01 via Congressional New Start approval

Projected Date for Completion of Phase; 30 Sep 03 and of Project 30 Sep 2010.

Teleport is reviewed by the Procurement Executive for DISA.

Date of Last Acquisition Decision Memorandum (ADM): NA

Project is in \_\_\_\_\_ PHASE or MILESTONE, Approval Dated: \_\_\_\_\_ Phase as of current review.

The Teleport program is approaching its first official milestone review on/about 05 Apr 02. Due to the maturity of the technology which will be utilized by the Program, entry into the DoD Acquisition Framework will be at Milestone C/Full Rate Production.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?  
Yes ☒ No ☐
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: +/-5%
3. Has DoD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐  
DISA CIO reviewed and certified compliant on 9 Jan 2002. Currently under review at Office of the Secretary of Defense (OSD) C3I.
4. Does this initiative implement electronic transactions or recordkeeping? Yes ☐ No ☒
5. If Yes was this initiative included in the GPEA strategic plan? Yes ☐ No ☒
6. Was a privacy impact assessment performed on this project? Yes ☐ No ☒

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
No.
3. How were the resource costs determined (CAIG, other costing methods, etc)? Resource costs were determined via use of an OSD reviewed Cost Model formulated specifically for the Teleport program and determined to be sufficient via independent evaluation.
4. Federal Financial Managers Improvement Act (FFMIA)
  - Is this project a part of the DoD Financial Management Architectural Improvement Process. Yes ☐ No ☒
  - Is this project categorized a Financial management or Financial Feeder System. Yes ☐ No ☒

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions				
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 - FY 2007
<b>Planning</b>					
APPN or Fund 1 to n - DevMod		4.500	14.212	6.678	16.435
Total Dev Mod		4.500	14.212	6.678	16.435
<b>Full Acquisition</b>					
APPN or Fund 1 to n - Dev Mod		2.000	96.675	53.542	148.985
Totals Dev Mod		2.000	96.675	53.542	148.985
<b>Maintenance/ Current Services</b>					
APPN or Fund 1 to n - Current Services		0	4.708	22.004	97.839
Totals Current Services		0	4.708	22.004	97.839
<b>Totals Resources by FY</b>		6.500	115.595	82.224	263.259
					467.578

Note: Due to PE consolidation within DISA, the STEP program funding is included in the Teleport funding summaries above. In FY 02, STEP represents 3% of the funding, in FY03 STEP represents 17% of the funding and in FY04, STEP represents 8% of the funding. FY01 STEP funding was reported under PE26 and is not included in the FY01 \$ reported above. Teleport received reprogrammed funding in September FY01 after New Start Approval which is reflected under the current Teleport PE10 along with STEP funds.

## Part II: Justification and Other Information

### A. Description

Description. The Department of Defense (DoD) Teleport system consists of the upgrade of a collection of existing telecommunication capabilities at selected Standardized Tactical Entry Point [STEP] sites. The system will provide deployed forces with sufficient interfaces for multi-band and multimedia connectivity from deployed locations anywhere in the world to online Defense Information System Network (DISN) Service Delivery Nodes (SDN) and legacy tactical command, control, communications, computers, and intelligence (C4I) systems. This system will facilitate the interoperability between multiple satellite communications (SATCOM) systems and deployed tactical networks, thus allowing the user a seamless interface into the DISN and legacy C4I systems.

The objective DoD Teleport facilities will integrate: C, X, Ku, commercial and military Ka-band satellite capabilities, Ultra High Frequency (UHF), Extremely High Frequency (EHF), Low Data Rate (LDR), Medium Data Rate (MDR), Advanced EHF, L-band, and High Frequency (HF) capabilities to provide connectivity for deployed tactical communications systems. The facilities will provide worldwide, integrated communications nodes that also have the ability to modularly insert emerging systems adopted by DoD to support deployed forces and Joint Task Forces (JTF). Teleport capabilities will be deployed incrementally in a multi-Generational FY01-FY10 program. Generation One will field capabilities for C, X, Ku, and UHF bands. The Generation One requirements for EHF (LDR, MDR), L, and HF bands were deferred to Generation Two for implementation. Generation Two will add military and civilian Ka bands. Generation Three will focus on advanced SATCOM systems to include the Advanced Wideband System, Advanced EHF, and Advanced Narrowband System.

The DoD Teleport Program has been designated as a Major Automated Information System (MAIS) ACAT-1AM program with ASD(C3I) serving as the Milestone Decision Authority (MDA). ASD(C3I) Designation Memorandum dated 05 May 2000 identifies the Defense Information Systems Agency (DISA) as the Executive Agent (EA) for the DoD Teleport Program. The EA has established a Teleport Program Office (TPO) to provide centralized management and oversight for the total Teleport program. The EA is responsible for the design, development, acquisition, and fielding of DoD Teleport systems that will satisfy JROC validated operational requirements.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

Teleport will provide seamless access to the DISN which supports the DoD/Joint Staff/DISA goals associated with C4I for the Warrior, Vision 2010 and Joint Vision 2020, by providing a global, secured interoperable information transport infrastructure in support of the Department's mission and mission needs

DISA carefully examined and reengineered business practices (as appropriate) as a basic tenant of the DoD Teleport Program. COTS hardware and software (with built-in commercial business practices) will serve as the backbone of the DoD Teleport System solution. The program expects to utilize the commercial sector to its fullest. This system shall take maximum advantage of commercial products, technologies, and non-development items. Industry proprietary components will be avoided to the maximum extent possible. This system will be designed using open systems standards to facilitate insertion of emerging technologies. The DoD Teleport Program, in addition to IT system acquisition, includes modernization of DISA business practices to align with best commercial practices whenever possible. It is believed that DISA, with the support of the commercial sector, will be the most effective organization to modernize their business practices. Manning required for the control, operations, and maintenance of the DoD Teleport Systems may consist of military, government employees, and contractor personnel. However, there will be no net increase in Military Service end strengths to control, operate, and maintain DoD Teleports. It has not yet been determined whether the private sector or the government can most effectively conduct long-term operations and maintenance of the Teleport System.

The functions DISA expects to perform through the DoD Teleport Program were determined to be so integral to the DISA mission that DoD Teleport has been identified by DISA as the system to satisfy the requirements of the C4I and Space-based Systems section of the Defense Planning Guidance and the Joint Requirements Oversight Council (JROC) validated requirements from the DISN Mission Needs Statement (MNS), dated 30 March 1995 and the DISN Capstone Requirements Document (CRD), dated 15 April 1996. Specifically, the DoD Teleport Program concept responds to the DISN MNS requirements to provide integrated connectivity to all theater and tactical elements and joint and combined interoperability in all mission areas to facilitate Combined and Joint Task Force (CTF/JTF) operations. The DoD Teleport system directly supports the DISN CRD requirements of Global Coverage and Connectivity, Interoperability, Responsiveness, and Technology Insertion. DoD Teleport also supports the DOD/Joint Staff/DISA goals associated with C4I for the Warrior and Joint Vision 2010, by providing the interface capabilities between the Long-haul infrastructure and the deployable service assets, which form the DISN Deployed Block. This ensures a global, secure interoperable information transport infrastructure in support of the Department's mission and mission needs.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

When information superiority is the main weapon in the national strategy, then management of that resource is an inherently governmental function. The purpose of DoD Teleport is to eliminate the need for last-minute contracts by providing pre-positioned satellite connectivity, a means to aggregate and crossband the signals, and connect the deployed units to the DISN. The DISN carries the GCCS, the GCSS, and other critical communications. The management of the crossbanding and connection to the DISN encompasses much more than routine operations and maintenance functions; it requires, on a daily basis, a value judgment. The DoD Teleport Program entails information management decisions that require seasoned decision-making capability and value judgments with potentially serious impact to deployed units. A Government official (would range from a system operator to a CinC) will be required to make decisions or take actions to:

- Protect the DISN from network attacks (virtually on a daily basis)
- Prioritize which frequencies will receive transmissions in the event of a limited bandwidth situation
- Prioritize which units or frequencies will be crossbanded with others
- Prioritize frequencies or information to combined forces and others.

Deployed warfighters rely on satellite-based communications for both tactical battlefield communications and for national command and control. The decisions made at the DoD Teleport facilities would have grave consequences in the event of war. This function is inherently governmental, and DoD Teleport supports core mission functions that need to be performed by the government.

DoD Teleport is an improvement to a mission critical system that integrates non-developmental commercial capabilities into an existing open architecture consisting of commercial leases and Government Furnished Equipment (GFE). This integrated solution meets mission needs, reduces costs, and improves overall effectiveness. Carefully selecting the networking technology used widely in the Telecommunication industry will afford a network that is supportable, maintainable, and interoperable into the future. The insertion of new technology will be coordinated across the DISN infrastructure blocks (Camp/Post/Station, Long-Haul, and Deployed) to ensure that interoperability and the efficient delivery of services to the end user meet operational requirements and are compliant with the GIG common operating environment (COE) architecture. DISA will capitalize on emerging technologies and innovative solutions to enhance DoD Teleport's ability to meet the Warfighter's needs, while reducing DoD costs and improving quality of service.

**B. Program Management/Management Oversight:**

Process Owner: Department of Defense in support of military missions by providing a consolidated, coherent system of pre-positioned gateways and multiplexers to assure access to the Defense Information Systems Network (DISN) for DoD warfighters.

Executive Agent: Defense Information Systems Agency (DISA)

Program Manager: CAPT Robert B. Leininger, USN

Contracting Offices: DISA Information Technology Contracting Office, National Capital Region (DITCO NCR), U.S. Army Communications Electronics Command (CECOM), PM-DCATS, Fort Monmouth, NJ, U.S. Navy Space and Warfare Center (SPAWAR), San Diego, CA

This project uses the Integrated Project Teams approach. Per Assistant Secretary of Defense C3I guidance, an Overarching Integrated Product Team (OIPT) was formed to formulate acquisition recommendations to the Milestone Decision Authority (MDA). In support of this OIPT, the EA (also the chair of the Integrating Integrated Product Team (IIPT)) determined that six Working-Level Integrated Product Teams (WIPTs) were required to support the IIPT/OIPT. WIPTs which support Teleport include: Configuration Management, Test, System Design, Implementation and Integration, Logistics, and Cost and Contracts.

**C. Acquisition Strategy:**

The Teleport Acquisition Strategy was developed using policy and guidance found in DoD Regulation 5000.2-R, 10 June 2001, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) and DoD Instruction 5000.2, Change 1, 04 January 2001, Operation of the Defense Acquisition System. It has been tailored to specifically meet the needs of the Teleport Program.

As approved by ASD(C3I) memo, Acquisition Guidance for the Teleport Program, dated 10 July 2001, the Teleport program will use a evolutionary acquisition process to incrementally provide Teleport system capabilities. Each succeeding phase of the Teleport program will expand upon the preceding Teleport development. Each increment of the program will provide additional access bandwidth, frequency bands and baseband improvements. The performance capabilities required in each phase shall be based on the Operational Requirements Document (as approved and modified by the JROC).

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

DISA plans to acquire Teleport equipment and infrastructure using existing contract vehicles to the maximum extent possible. DISA/DISN contract vehicles for terrestrial connectivity, and other DoD or Government-wide contracts/ordering vehicles for acquisition of the earth terminals, baseband equipment and facility/site upgrades. The performance requirements of the DoD Teleport system are based upon proven technologies and off-the-shelf equipment. Technology development, or utilization of Small Business Innovative Research (SBIR) or other R&D contracts, is not contemplated. The Teleport Program Office (TPO) will designate a single procurement agent for each piece of common equipment using existing Service contracts for procurements to the maximum extent possible. The analysis of contracting options takes into consideration program, technical, and cost risks associated with particular contract types.

The primary challenge facing this acquisition is coordinating service provisioning from a number of different contracts in a timely and cost effective manner.

Teleport contracting activities at a given site during each generation will center around four major system elements:

- Terrestrial tail circuit connectivity.
- Earth terminals.
- Site baseband and associated peripheral equipment.
- Facilities and site upgrades

Strategies for each element are discussed in the following paragraphs.

#### Terrestrial Connectivity

Provision has already been made for obtaining terrestrial tail circuits and associated services for most of the global DISN. The following ID/IQ Contracts, all competitively awarded, will be used for acquiring these services:

- DISN Transmission Services – CONUS (DTS-C) – Contract DCA200-97-C-0048 awarded to AT&T in January 1997
- DISN Transmission Services – CONUS Extension (DTS-CE) – Contracts DCA200-99-D-0050, 0051 and 0052, awarded March 1999 to AT&T, MCI and SPRINT.
- DISN Transmission Services – Pacific (DTS-P) – Contract DCA200-00-D-5000, awarded October 1999 to MCI
- Hawaii Information Transfer System (HITS) – Contract DCA300-97-D-0002 awarded to AT&T in February 1997

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

- DISN – Europe – While there is no omnibus transmission services vehicle in Europe comparable to the DTS-P contract, the DISN infrastructure in Europe provides standardized avenues for obtaining transmission services for sites in Europe.
- DISN Network Management Support Services – Global/Network Engineering (DNMSS-G/NEC), Contract DCA200-99-D-5011 with DynCorp.
- DISN Network Management Support Services – Global/Associate Support (DNMSS-G/ASC), Contract DCA200-99-D-5015 with Artel,

DISA plans to provide all voice and data circuits. The majority of Teleport terrestrial requirements will be provisioned using one of the contract vehicles described above; any other requirements will probably be provisioned via competitive offers on the DITCO acquisition bulletin board system (DABBS).

Earth Terminals

Existing contract vehicles are the primary choice for acquiring Teleport earth terminals. Existing vehicles to be used include:

- Commercial Satellite Terminal Program (CSTP) – CSTP, managed by the US Army at Ft. Monmouth, is currently DISA's principal source for obtaining commercial C, Ku and Ka band commercial earth terminal equipment. The CSTP has Blanket Purchase Agreements (BPAs) with eight different companies supporting one or more of five commercial earth terminal equipment segments. These five segments cover most relevant commercial product lines. The segments are as follows:

1. Large fixed size earth terminals
2. Deployable earth terminals
3. Transportable earth terminals
4. Mobile terminals (INMARSAT, etc.)
5. X-band commercial terminals (the DSCS certified portion of our tactical tri-band terminals).

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

The following is a matrix of the BPA holders listed by segment:

	1	2	3	4	5
DataPath	X	X	X	X	X
L3 Communications	X	X	X		X
ETS	X	X	X		
Hughes				X	
SpaceLink	X	X	X	X	X
Spectrum				X	
AIS	X	X	X		
ITT Industries	X	X	X		X

Many of the BPA holders are small businesses. BPAs are awarded competitively and result in a best-value, FFP delivery order. The standard warranty is one year. The BPAs include options for extended warranty/maintenance provisions that have historically been priced between 4-6% of the equipment purchase per year. The antenna is the pacing long-lead item of 120 days. The agreements are revised annually to encourage admission of new, interested businesses and allow dismissal of businesses no longer interested. Proposal and award time for orders is 3 weeks. The ceiling per task order is \$5M.

SPAWAR's DMR program, Contract N00039-98-D-0029, is currently identified as the most likely source of off-the-shelf UHF terminals for Generation One. The schedule viability of DMR terminals continues to be evaluated by the TPO. Additional EHF terminal contract vehicles may be investigated. All of the other MILSATCOM systems being integrated into Teleport sites will have current or planned acquisition vehicles for their earth terminal segments; the TPO will coordinate with those programs at appropriate points during the Teleport implementation program.

DISA expects to procure Generation Two EHF terminals from the following contract vehicle or its successor:

- Navy EHF SATCOM Program Low Data Rate (LDR)/Medium Data Rate (MDR) Follow on Terminal, Space and Naval Warfare Systems Command (SPAWAR) Contract, N00039-98-C-0047. This contract provides for EHF MDR terminals meeting Teleport Generation Two requirements.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

Teleport system users will be responsible for the acquisition of space segment bandwidth to support their own requirements. Users will obtain: 1) approval to use military satellite bandwidth through the established channels for a given system, and 2) commercial bandwidth, through the Commercial Satellite Systems Office (CSSO) or other contract vehicle, on a pay-as-you-go basis.

Baseband & Other Peripheral Site Equipment

Provisioning procedures already in use at STEP/other similar sites will be utilized to obtain modems, multiplexing equipment, switches, crypto gear, and other peripheral equipment that is required to make Teleport earth terminal equipment operational. The PM-DCA TS organization currently procures much of this equipment. This equipment is currently ordered through a variety of avenues, including General Services Administration (GSA) schedules, National Security Agency (NSA) schedules (for crypto gear), and other contracts or basic ordering vehicles. For each site, during each Generation of the Teleport implementation program, the TPO will develop required order lists or bill of materials (BOM) for use in obtaining required site equipment. The table below summarizes current information on available provisioning vehicles for baseband equipment relevant to the Teleport program.

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency (DISA)

Contractor	Contract Vehicle	Contract Expiration
Raytheon	DAAB07-97-C-D014	May-02
Comtech EF Data	FA 2550-01-G-0004	Jun-04
L3	GS00T00NSD0010	Dec-02
NET	DCA 200-01-A-5002	Jun-02
General Dynamics	DAAB07-97-D-F758	Mar-02
Group Tech.	MIPR to NSA	Oct-06
Comtech EF Data	Navy Furnished	Jun-04
Truetime	GS-24F-1477C	CY2004
DNE	DAAB07-01-D-A019	Dec-06
Inrange	Coastal Systems	5 yrs
Cornet	CECOM DAAB07-00-D-H753	Sep-03

In the event of any unique requirement that is not in the scope of existing contracts, the TPO or designated agent will initiate a new procurement using the most appropriate acquisition strategy. The use of best practices, e.g., Performance Based Contracting, Multiple Awards, Use of Past Performance, etc., will be considered. The TPO will consider all prospective sources of supplies and/or services that can meet the need, both domestic and foreign. Commercial and non-development items shall be considered as the primary source of supply. Consideration will be given to the national policies on contracting and subcontracting.



**D. Alternative Analysis and Risk Management:**

Cost/benefit analysis. An economic analysis including cost benefit analysis and Return on Investment (ROI) calculations were recently performed for the Teleport Generation One (GEN 1) system. The ROI divides the expected benefits (O&S savings) by the investment costs. The numbers are solid. Generation One uses non-developmental equipment, so the investment costs are hard numbers (the denominator). The Economic Analysis found that DoD Teleport Program Generation One would produce a return on investment of 2.68. In other words, every dollar invested in DoD Teleport would save DoD \$2.68. In addition to the cost benefits, the DoD Teleport Program will produce significant operational benefits that have an economic consequence. The operational benefits of DoD Teleport are clear. Operational benefits include more data capacity, satellite bands, geographic coverage, frequency options, and interoperability. Military satellite communications are saturated, and DoD Teleport builds the gateway infrastructure for the next generation of satellite communications. The operational benefits of DoD Teleport are so great that most CINCs have made it a priority in their Integrated Priority Lists (IPL). The DoD Teleport will give our warfighters the ability to communicate quickly and securely throughout most of the world and exchange information with units with whom they cannot communicate today.

Analysis of alternative options. DoD directs a hierarchical approach to identifying solution alternatives. The first part of this approach is to consider non-material solutions and then material solutions. Numerous policy and procedural measures have been undertaken to improve the effectiveness and efficiency of fielding and providing C4I connectivity capabilities for the Warfighter. Policies and procedures, to include DoD Directives, Defense Management Review Decisions, and Chairman of the Joint Chiefs of Staff instructions, that impose interoperability considerations on all new systems and mandate the use of standards, have been published. However, progress toward the required DoD-wide end-to-end integrated capability has been slow. Additionally, the existence of legacy systems and the need for CINCs, Services and Defense agencies to retain the costly, dedicated transmission systems have resulted in only marginal improvements in end-to-end C4I connectivity capability and savings. Today's Warfighters' missions, economic realities, and technology breakthroughs demand faster improvements for C4I systems connectivity and support therefore non-material solutions cannot satisfy the user requirements. Consequently, There are three material alternatives for meeting this need:

- a. Alternative 1 - Maintaining the "status quo" of loosely coordinated development, implementation, and management of Service and Defense agency systems (special purpose and common-user) that require special interfaces to achieve the interoperability and integration to support joint operations. Major common-user systems that require interfacing include, the Defense Switched Network, Defense Data Network, AUTODIN, Defense Simulation Network, Defense Red Switch Network, Defense Special Security Communications System, and the national Secure Telephone System. Special purpose systems with partial or dedicated transmission



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

- and network management that must be interfaced include Service and agency router networks, dedicated intelligence Community networks, and dedicated CINC C2 support networks.
- b. Alternative 2 - Simultaneously upgrade all department switching/transmission and network systems to standard state-of-the-art platforms.
  - c. Alternative 3 - Incrementally integrate all DoD network and transmission systems into a secure, seamless, standards based, information transfer infrastructure with responsible DoD activities at local, regional, theater and global levels, and tactical interfaces, performing integrated management. Stay in step with evolving commercial technology and standards via planned technology insertion, thereby avoiding use of "proprietary" hardware and software solutions and their related pitfalls.

Since the status quo was determined not to be able to meet future requirements, the Feasibility Study utilized the second and third material alternative solutions in developing the architecture alternatives.

If the decision is made to pursue an acquisition program, the acquisition decision-makers shall observe the following hierarchy of alternatives:

- a) The procurement (including modification) of commercially available systems or equipment, the additional production (including modification) of already-developed U.S. military systems or equipment, or Allied systems or equipment;
- b) Cooperative development program with one or more Allied nations;
- c) New joint Service development program; and
- d) A new Service-unique development program.

Teleport utilizes commercial products. Some of the rationale for not selecting the other alternatives is described below. Because of the nature of the Teleport System, a combined development program is not required because the design capitalizes upon both COTS networking technologies and equipment used by tactical Warfighters. A joint program is also not applicable as DISA functions are already inherently joint in nature. This leaves the alternatives of utilizing COTS products (preferred) and building a unique system. A unique system is not a required option in this case since in order to satisfy the order of magnitude in growth, two fundamental tenets must be observed: commonality and standardized, proven equipment configurations.

Teleport is an improvement to a mission critical system that integrates non-developmental commercial capabilities into an existing open architecture consisting of commercial leases and GFE. This integrated solution meets mission needs, reduces costs, and improves overall effectiveness. Carefully selecting the networking technology used widely in the Telecommunication industry will afford a network that is supportable, maintainable, and interoperable into the future. The insertion of new technology will be coordinated across the DISN infrastructure blocks (Camp/Post/Station, Long-Haul, and Deployed) to ensure that interoperability and the efficient delivery of services to the

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

end user meet operational requirements and are compliant with the DII common operating environment (COE) architecture. DISA will capitalize on emerging technologies and innovative solutions to enhance Teleport's ability to meet the Warfighter's needs, while reducing DoD costs and improving quality of service. DISA developed a detailed set of functional requirements from the DISA System Required Capabilities to meet the joint Warfighter's needs. DISA felt confident that commercial could meet the essential Joint requirements set forth in JROC Memorandum 140-00.

The architecture alternatives described below are a combination of the second and third (simultaneously upgrade and incrementally integrate) Material Solutions and the results of the Hierarchy of Material Alternatives determination (utilize commercial products) described above. The following is a synopsis of the alternatives considered in the DoD Teleport Architecture Feasibility Study and hence the AOA.

As a rule, the elements that comprise each architecture are held constant across all of the architecture alternatives including the time phasing of equipment, the terrestrial connectivity costs, the master list of equipment, and a dual redundant core ATM switching fabric. This has been an essential tenet of the Teleport feasibility analysis, as it promotes a fair and representative cost of the five architectural approaches. A brief overview of each architecture considered in this study follows:

The fundamental approach, in the centralized architecture #1 (most expensive), is based on collocating all required assets within the same LAN and facility. All of the elements described earlier are within a local span of control and monitoring. The six sites are Ft. Buckner, Wahiawa, Camp Roberts, Northwest, Landstuhl/Ramstein, and Lago di Patria.

Architecture alternative #2 (least expensive) has some of the same features as architecture #1, in that both centralize the base band multiplexing and ATM switching/routing; however, the ETs are implemented as distributed elements and only four core sites (Ft. Buckner, Wahiawa, Northwest, and Lago di Patria) are employed. Landstuhl/Ramstein and Bahrain are supporting sites.

Architecture #3 (third most expensive) has two major improvements over architecture #2: (1) fault tolerance and (2) cross banding. The fault tolerance is provided via a surge package that can be applied to any of the six sites: Ft. Buckner, Wahiawa, Camp Roberts, Northwest, Landstuhl/Ramstein, and Lago di Patria. Each of these six sites will be equipped with a large core ATM switch and the requisite base band equipment. The cross banding is improved by the additional base band Multiplexer Integration and DCSS Automation System (MIDAS) equipment and ATM core switch that have been added for fault tolerance.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

Architecture #4 (second most expensive) is a hybrid that possesses the performance and fault tolerant advantages of architecture #1 at a fraction of the FY02 and FY03 costs. It employs a time-phased build-up of the system, starting with four Teleports in 2004 and adding two more in 2007. The core Teleport ATM switching/routing and base band equipment infrastructure is installed at five of the six primary Teleport sites: Ft. Buckner, Wahiaawa, Northwest, Landstuhl/Ramstein, and Lago di Patria. Each of the primary sites is sized to handle 67% of the 2010 SSC traffic in the first phase of build-up and all six sites handle 100% of the 2010 SSC by Full Operational Capability (FOC).

Architecture #5 (fourth most expensive) is identical to architecture #4, with the exception that the phased capacity of the Teleports differ. The core Teleport ATM switching/routing and base band equipment infrastructure is installed at five of the six primary Teleport sites: Ft. Buckner, Wahiaawa, Northwest, Landstuhl/Ramstein, and Lago di Patria. At Initial Operation Capability (IOC), the Warfighter has a minimum of two Teleports in view, and the equipment is sized to satisfy 67% of the 2010 SSC capacity. As in alternative #4, fault tolerance is achieved by growing the equipment at Camp Roberts, Landstuhl/Ramstein, and Bahrain so that by 2007 all six sites are equally sized to 67% of the 2010 SSC capacity. Note the original primary Teleport sites: Ft. Buckner, Wahiaawa, Northwest, and Lago di Patria remain unchanged; no additional equipment is added after IOC. Instead, at FOC (2007), the Warfighters will connect via three Teleport sites to satisfy MTW. CMTW is accommodated by six Teleports.

Based on the results of the Architecture Feasibility Study, the JROC concluded that Alternative #5 was the best value alternative. Although it cost slightly more than the least expensive option, it would prevent costly leased lines. Alternative #5 provides the most robust support to the warfighter, operational suitability, and cost compromise. The JROC approved alternative #5 for program implementation because it meets the triangulation requirements of the satellite orbital paths while leveraging robust existing facilities Wahiaawa, Camp Roberts, CA, Lago Patria, Northwest, VA and Ramstein Landstuhl.

Underlying assumptions utilized in conduct of the economic analysis included those describing the present and future environment upon which an economic analysis is based and are made to support, and reasonably limit, the scope of a study. The following general assumptions were made in order to develop estimates for the Status Quo and the selected Teleport GEN 1 Program Alternative.

1. Gen One of the Teleport Program will be complete in FY03.
2. Systems for all alternatives will be built upon existing sites.
3. Terminals will be purchased as opposed to leasing and will be comparable in size and performance in both alternatives.  
Facility, utility, and software requirements for both alternatives will be comparable.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

Estimate of Risks. The DoD Teleport program employs an aggressive and rigorous risk management process that is documented in the DoD Teleport Risk Management Plan (RMP) (Draft). The RMP describes how program risks will be identified, tracked, and mitigated, and focuses in three areas: cost, schedule, and performance. The Teleport risk management includes the establishment of a single focal point, a Risk Coordinator, within the TPO with the responsibility for overseeing the Teleport risk management process.

The Teleport RMP details the risk management process and supporting procedures that:

- Identifies the individual risk items.
- Documents the risk item information, including risk rationale, on the individual Risk Information Forms (RIF).
- Categorizes the risks in terms of cost, schedule, and/or performance/technical risk.
- Rates the risks as high (red), medium (yellow), or low (green) based on a numeric weighting matrix with consequence/program impacts and likelihood/probability intersections.
- Identifies opportunities for risk mitigation.
- Monitors the risk items as the program proceeds.
- Reports on status and results.

#### Cost Risks

Cost risks relate to the uncertainty of the ultimate actual program costs. The uncertainty results from unknowns regarding the cost of technology, equipment, installation, operations, etc. and from budget issues including the availability and appropriate level of funds to accomplish the program efficiently and economically. Other schedule and performance/technical risk issues also impact cost uncertainty.

Teleport cost risk for Generation One (i.e., technology and equipment) is considered low as proven technology and Commercial Off-the-Shelf (COTS) equipment is being used. Implementation (e.g., installation and site preparation) costs, especially at Outside the Continental United States (OCONUS) sites, are less certain and are medium risk. Budget-wise insufficient funding (i.e., medium risk) will cause program delays and possibly the use of alternative program implementations that may be less efficient and more costly. Cost is also less certain for Generations Two and Three (due, in part, to the later time-frame) with an increase in cost risk.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

**Schedule Risks**

Schedule risks are concerned with time adequacy to begin, complete, and/or accomplish the particular activity or event to meet the objective milestone(s). This includes ordering and receipt of equipment in time for site installation, Host Nation Approvals (HNA) for site work to start, and actual durations for site preparations, installations, testing, etc.

The primary schedule risk is the attainment of the Generation One Initial Operational Capability (IOC1) per the ORD. Given various program delays, most specifically having to do with obtaining Congressional New Start approval for the program, the IOC1 date must now fall in late CY2003. Many activities must be accomplished to meet that date. A number of site implementation activities must occur in parallel to achieve this date. This parallel implementation is a high risk. Mitigation techniques (e.g., multiple implementation teams) require more resources at any point in time. Additional schedule risks also arise from the interrelationship and dependence on related programs – MIDAS, Gapfiller, Advanced Wideband, and Advanced Narrowband.

**Performance Risks**

Performance (i.e., technical) risks deal with the ability to successfully meet requirements through: technology; design; configuration; equipment characteristics, features, functions; interfaces; integration; installation; etc.

The ASD(C3I) Acquisition and Management Guidance recommends use of existing Service contracts for procurements. The communications requirements are based on proven technologies and rely on existing and planned DISA contracts that are part of the global DISN and other existing Service contracts. The principal performance risks for Teleport are its Generational implementation program and dependence on the success of numerous other satellite technology development programs (e.g., Wideband Gapfiller System, Advanced Wideband System, Advanced Narrowband System, Advanced EHF, and MIDAS). Although a non-developmental COTS alternative to MIDAS is currently being considered, the capabilities and successful implementation of Teleport are ultimately dependent on the performance of these other programs.

**Risk Mitigation**

Teleport risk mitigation employs the accepted risk handling techniques of assumption, transfer, control, and avoidance as detailed in the RMP. Approximately 40 risk items were identified and categorized as Cost, Schedule, and Performance/Technical. Assessment and mitigation for risk items are currently under development. Specific definitions for the risks relevant to the Teleport program have been identified in Appendix A of the Teleport Risk Management Plan.

**E. Enterprise Architecture and Infrastructure Standards:**

Does this system meet current Government wide, DoD and Agency interoperability requirements? Describe current compliance levels, target levels, and date target will be accomplished. (Map to agency's technology vision.) The Teleport program is ensuring that all baseband hardware used within the Teleport has received interoperability certification testing within the Joint Interoperability Test Component (JITC). Most of the Teleport hardware is already in use by the Standardized Tactical Entry Point (STEP) program or by deployed warfighters. As a result, most of the equipment has already received interoperability certification. For new equipment types, such as ATM, the Teleport Program is performing the interoperability certification on the new equipment.

Infrastructure Strategy: The Teleport Program will provide pre-positioned DISN services for the warfighter. We are in coordination with the appropriate DISN programs to ensure the proper level of services for the deployed warfighter.

Are HW requirements included in this funding? If no, by what means is the hardware provided? HW requirements are included in this funding.

Transport (Communications and Computing) requirements are met by what means? The Defense Information Systems Network (DISN) is the primary means of transport to the various services.

What are the interdependencies with other acquisitions (such as base level infrastructure requirements? The Teleport Program is dependent on several other programs, and is ensuring synchronization with these programs through the Teleport I&I Team. Other programs include (Wideband Gapfiller, Milstar, MUOS, Advanced Wideband, Advanced Narrowband, DSCS 52-Mod Upgrade Program).

Is this system based on COTS; mix of COTS and custom, or custom only. Provide justification for custom components? The Teleport is built (as per the ORD) on a mixture of COTS and GOTS products. The Teleport doctrine is to not rely on developmental products.

Describe the Data Architecture approach? The Teleport provides pre-positioned services for NIPRNET, SIPRNET, JWICS, DRSN, DSN, and VTC. Each of these services represent a different combination of voice and data services. NIPRNET and SIPRNET are non-secure and secure, respectively, IP networks. DSN and DRSN are non-secure and secure, respectively, voice networks. VTC is a direct and dial-up (ISDN) video services. JWICS is a secure (INTEL) data network for which Teleport acts as a transport mechanism. The Teleport provides access to each of these services for the variety of multiplexing platforms currently used by the individual Services.



Describe the Functional (Mission or Component) Architecture approach? The overall mission of the Teleport is to provide an interoperable interface into strategic networks via pre-positioned services for the warfighter over a variety of satellite communications avenues (C, Ku, X, UHF, EHF, X, AEHF, ANS, AWS). In order to support the warfighter, the Teleport provides access to a variety of different component types that are currently in use by the Services in addition to new component types (ATM) that offer interoperability among all Services.

#### **F. Security and Privacy:**

Describe the Security approach (Defense in Depth). The defense in depth security approach employs protection mechanisms in a layered fashion, at multiple locations in the system architecture. This ensures the Teleport system maximizes resistance to attacks and minimizes the probability of a security breach due to a weakness (known or unknown) in any single security mechanism.

It is important to note that the zones of defense may be logical and not necessarily physically separate. It should also be noted that the selection, placement, and configuration of particular security mechanisms are implementation dependent. The type and strength of security mechanisms are driven by the information protection requirements for a particular information systems classification.

Teleport plans on implementing a layered security scheme to protect monitoring and control, as well as, network interfaces which includes Intrusion Detection Systems at different points, Firewalls and Access Control Lists. Some Teleport security will be provided by accessing existing security systems.

Privacy assessments for this initiative. COTS VPN mechanisms used for encryption of unclassified data, and of classified data that will be handled at its original level. To provide for interoperability, IPSEC based mechanisms will be used if available. IPSEC mechanisms will utilize 3DES for encryption.

Discuss enabled for use with the DoD Common Access Card? If no, when will it be? No, not applicable. NIPRNet Internet firewalls that require the use of public key certificates shall comply with the Department of Defense (DoD) Security Management Infrastructure (SMI) and Public Key Infrastructure (PKI) guidance. Teleport will support this requirement in its Firewall configurations.

**F. Government Paperwork Elimination Act (GPEA)** Teleport is a satellite gateway system. GPEA does not apply.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

Performance Based Management System (PBMS) Which Performance based management system will you use to monitor contract or project progress? Modified Earned Value Management System (EVMS) procedures and reporting, as described in the appendices to DoD 5000.2-R, may be used for Teleport at the program level given that no prime contractor for the Teleport system is contemplated. However, the Teleport program office will develop budget and schedule baselines for those program elements that will be accomplished by DISA and for those that have been delegated to other DoD organizations. These baselines will be structured around the program Work Breakdown Structure (WBS) and provide a description of the work packages to be accomplished, an associated schedule with milestones, and the concomitant required funding. Cost and schedule performance will be monitored for those elements via tailored reporting from the program office and the other implementing DoD organizations.

The TPO will make use of whatever performance management and metrics mechanisms are in-place to monitor performance on existing contract vehicles used to implement Teleport. If any new contracts are let specifically for Teleport, they will incorporate those contractor performance management provisions that are appropriate for the contract size and type.

**B. Original Baseline:**

Teleport is in the process of establishing its original baseline which will be presented and approved by the Milestone Decision Authority (MDA) at the upcoming Milestone C/Full Rate Production meeting currently scheduled for early Apr 02.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

**C. Current Baseline Information:** N/A

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
a. Previous Baseline:						
Cost Goals (\$M)						
Schedule Goals (milestones)						
b. Current Estimate:						
Cost Goals (\$M)						
Schedule Goals (months)						
c. Variance from Baseline Goals:						
Cost Goals (\$M)						
Schedule Goals (months)						

**D. Actual Performance from Approved Baseline:**

The work planned and budget amounts will be determined when initial baseline is established.

Measurable performance benefits or goals for this segment or phase of this initiative.

FY 2001: Congressional New Start Approval Gained (20 Sep 01)

FY 2002: Complete ACAT 1A documentation requirements and attain Full Rate Production (FRP) Milestone Decision (MD). Procure hardware, which will provide C and Ku band capability to the deployed warfighter during Teleport Generation 1.

FY 2003: Implement C and Ku band operational capability at four Teleport sites (Initial Operational Capability (IOC1)) and procure hardware which will provide UHF capability to the deployed warfighter during Teleport Generation 1.

FY 2004-07: Implement UHF operational capability at four Teleport sites (Initial Operational Capability (IOC2)).

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency (DISA)

3. Cost and Schedule Corrective actions: None. Having just received Congressional New Start approval in the last ten days of FY01, Teleport is now actively engaged in gaining Milestone Decision Approval (MDA) for entry into the acquisition framework at Full Rate Production (FRP)/ Milestone C.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym Global Combat Support System (GCSS)  
Budget Initiative Number: 0882  
IT Registration System Number ADLIS08 (Section 8121, FY 2000 DOD Appropriation)  
Mission Critical Status: Mission Critical.  
Information Technology Project or National Security System: Information Technology  
Program Activity/Mission Area: Communications & Computing Infrastructure

### PROJECT STATUS:

Project Status: New ☐ Ongoing Yes ☒

Date Project was initiated: 30 September 1995

Projected Date for Completion of Phase: Ongoing; and of Project: N/A.

This project is reviewed by the DISA Procurement Executive.

Date of Last Acquisition Decision Memorandum (ADM): N/A.

On 14 March 01, received GCCS Configuration Management Control Board Limited (CMB) Fielding Decision to field GCSS (CINC/JTF) V2.0 as a GCCS mission application to PACOM, CENTCOM and JFCOM. On 14 September 01, the GCCS CMB gave a Global Fielding Decision to continue fielding GCSS (CINC/JTF) V2.0.

Project is in \_\_\_\_\_ PHASE or MILESTONE, Approval Dated: \_\_\_\_\_ Phase as of current review. N/A.

GCSS has been designated to be part of the Rapid Improvement Team (RIT) Pilot initiative in a memorandum dated 21 December 2001 by the DOD CIO & USD(AT&L). In support of the RIT Pilot initiatives, GCSS (CINC/JTF) will be testing a streamlined acquisition paradigm to rapidly deliver capabilities to the warfighter. As a pilot, the system is being treated as an ACAT IAC. During the pilot, the program will be monitored by DISA as the Component Acquisition Executive and by the RIT Pilot Team. The pilot project officially starts March 02.

No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?

Yes ☒ No ☐

2. Security mechanisms currently being implemented by the GCSS (CINC/JTF) to maintain the confidentiality, integrity, availability and accountability of the hardware/software and data associated with GCSS (CINC/JTF) include: access control utilization via unique access login ID, individual accountability through the use of DOD Public Key Infrastructure (PKI), workstation-level access control through DII/COE login mechanism, transaction activity logging via application clients and servers, the use of Secure Sockets Layer (SSL) and VirtualDB Transition Interface (VTI) to provide two-way authentication and encrypted communication between GCSS clients and servers.

3. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 12.5%

4. Has DOD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐  
CCA compliance is reviewed and briefed at DISA Annual Spend Plan reviews. The last annual review for DISA/GCSS was held 11 October 01.

5. Does this initiative implement electronic transactions or recordkeeping?

Yes ☐ No ☒

If Yes was this initiative included in the GPEA strategic plan?

Yes ☐ No ☐

If No, discuss in Part 2, Section G?

Was a privacy impact assessment performed on this project?

Yes ☒ No ☐

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
Yes, there were decreases to the program in the amended FY2002 Budget.
3. These decreases were agency wide based on OSD Congressionally mandated cuts.
4. GCSS uses a combination of analogy, actual and parametric cost methods to determine resource requirements.
5. Federal Financial Managers Improvement Act (FFMIA)
  - This project is not a part of the DOD Financial Management Architectural Improvement Process.
  - Is this project categorized a Financial management or Financial Feeder System.
  - FFMIA compliance is not applicable to GCSS

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions					
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 - FY 2007	Total
<b>Planning</b>						
APPN or Fund 1 to n - DevMod	76.713	24.156	18.131	19.681	83.849	222.530
Total Dev Mod	76.713	24.156	18.131	19.681	83.849	222.530
<b>Full Acquisition</b>						
APPN or Fund 1 to n - Dev Mod						
<b>Maintenance/ Current Services</b>						
APPN or Fund 1 to n – Current Services	25.337	8.401	12.258	11.677	50.416	108.089
Totals Current Services	25.337	8.401	12.258	11.677	50.416	108.089
<b>Totals Resources by FY</b>	102.090	32.557	30.389	31.358	134.265	330.619

Note: The cumulative numbers total FY2000 and Prior include EC Initiative funding thru FY1999. The total shown is not exclusively GCSS, but also includes 29M for EC/EDI through FY1999.....

## **Part II: Justification and Other Information**

### **A. Description:**

Description. Global Combat Support System (GCSS) is an initiative that provides end-to-end information interoperability across and between combat support functions and command and control functions. GCSS, in conjunction with other Defense Information Infrastructure (DII) elements including Global Command and Control System (GCCS), Defense Information Systems Network (DISN), Defense Message System (DMS), Defense Enterprise Computing Centers - Detachments (DECC-D), and CINC/Service/Agencies (C/S/As) information architectures, will provide the information technology (IT) capabilities required to move and sustain joint forces throughout the spectrum of military operations.

DISA is responsible for two main efforts within the GCSS Family of Systems (FOS). The first is System Architecture and Engineering for the GCSS FOS and the second is for development, integration, fielding, and operation and maintenance of Global Combat Support System (Commander in Chief/Joint Task Force) (GCSS (CINC/JTF)), which provides Combat Support (CS) information to the joint warfighter. GCSS (CINC/JTF) provides improved situational awareness by integrating CS information into the Command and Control (C2) environment and improves communications between the forward deployed elements and the sustaining bases, ultimately resulting in significant enhancement of combat support to the joint warfighter. GCSS (CINC/JTF) will significantly increase access to information as well as the integration of information across combat support functional areas. GCSS (CINC/JTF) and GCCS applications are available on the same workstation providing decision makers with command and control information as well as combat support information. Using web-based technology, GCSS (CINC/JTF) provides "any box, any user, one net, one picture" capability.

Statement of how this project helps the agency meet the agency/DOD mission; long term strategic goals and objectives (Mission goals and/or IT strategic plan.) GCSS supports three (3) of DISA's strategic goals, as follows: Provide a flexible, reliable information infrastructure capable of supporting the evolving Global Information Grid required by the warfighter and others to achieve the highest levels of effectiveness in joint and combined operations; easy sharing of high quality information supporting interoperability among the US Forces and Allies; Defense information resources are secure.

Describe the pre milestone 0/ Planning activities that lead up to this decision. Business Process Reengineering, Migration plan; other approaches. The GCSS foundation is built upon on a solid requirements foundation. On 30 September 95, the Program Decision Memorandum (PDM) II approved the GCSS initiative to provide the warfighter a fused, real-time true picture of the battle space and the ability to order, respond, and coordinate vertically and horizontally across the combat support domain. A Joint Staff validated Mission Needs Statement (MNS) dated 10 September 1997 establishes the military need for GCSS. The combat support requirements for the GCSS Family of Systems are identified in a JROC approved, Capstone Requirements Document dated 5 June 00). The Phase 3 GCSS (CINIC/JTF) Requirements Identification Document (RID) was approved by the Joint Staff in Dec 00. DISA also produced several prototype versions which were used at PACOM and during several exercises.

Basis for selecting the project, including demonstration that the investment is required for inherently government function; demonstrate that the work processes have been redesigned to reduce costs and improve effectiveness. GCSS (CINIC/JTF) program functions are inherently governmental since the program provides combat support to the warfighter. The program functions relate specifically to commanding military forces, federal employees, and federal procurement activities and are explicitly inherently governmental functions, performed by government officials.

#### **B. Program Management/Management Oversight:**

Identify the process owner (business activity, military mission), executive agent, program manager, and contracting office that manages this project if not, how is this project managed?

- Process Owner: Department of Defense, Joint Staff, J4
- Executive Agent: Defense Information Systems Agency (DISA)
- Program Manager: DISA, Global Combat Support System (GCSS) Program Office
- Contracting Office: DISA, Defense Information Technology Contracting Office

Does this project use Integrated Project Teams approach? If not, how is the project/initiative accomplishments monitored; how are resources reviewed. GCSS does not use formal IPTs. The Joint Staff J3, J4 and J6 provide functional and technical guidance on the GCSS development to ensure the interests of the Joint Community are met. The Joint Staff/J4 acts as the functional proponent for the GCSS (CINIC/JTF) and prioritizes joint requirements for the CINCs and Unified Commands. The GCSS Management Structure includes a General Officer Steering Group (GOSG) and Planners Board which provide the overall vision and direction for the GCSS FOS which includes the GCSS (CINIC/JTF).



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

The Joint Staff Director of Logistics chairs the General Officer Steering Group and provides the GCSS vision and course directions to DISA. Requirements are validated and prioritized by user groups and the Joint Staff before candidate technical solutions are identified.

**C. Acquisition Strategy:**

Identify major contract names; prime contractor and City, State, if awarded.

Base Technologies Inc., McLean, VA; Booz, Allen and Hamilton, McLean VA; Comtek, Sterling, VA;  
Computer Sciences Corporation, Falls Church, VA; Enterworks, Sterling, VA; FGM, Sterling, VA; Logicon, Arlington VA;  
UNISYS, Falls Church, VA; Dyad Sodality Inc. (DSI), Manassas, VA., and EDSI, Fairfax, VA.

Identify the type of contract and why it was chosen.

Base Technologies Inc., Time & Materials  
Booz Allen and Hamilton, Cost Plus Fixed Fee  
Communication Technologies, Inc., Time and Materials  
Computer Sciences Corporation, Time & Materials  
Enterworks, Time and Materials  
FGM, Time and Materials  
Logicon, Cost Plus Fixed Fee  
UNISYS, Firm Fixed Price  
Dyad Sodality Inc., Time and Materials  
EDSI, Time and Materials

The contract is not performance-based.

**D. Alternative Analysis and Risk Management: Describe AoA.**

Cost/benefit analysis (including return on investment (ROI), replaced system or process savings, recovery schedule and any intangible (mission) returns that benefit the organization/mission but are difficult to quantify. Product measures relative to the value of services offered and investments made (e.g., ROI) are currently being developed for GCSS. The effort involves the development of a GCSS (CINC/JTF) economic analysis that will identify life cycle costs. Benefits, and risks associated with current and upgraded GCSS (CINC/JTF) capabilities will be evaluated throughout the program.

Analysis of alternative options. (Describe preliminary activities if AoA not yet performed.)

A formal AoA was not performed at the Program's inception. In lieu of a formal AoA, the program office continues to evaluate technical alternatives throughout lifecycle of the program.

Underlying assumptions.

N/A

Estimate of Risks. Program is low risk due to use of proven commercial technology and integrated delivery through the use of existing GCCS policies, procedures, processes and infrastructure.

**E. Enterprise Architecture and Infrastructure Standards:**

Does this system meet current Government wide, DOD and Agency interoperability requirements? Describe current compliance levels, target levels, and date target will be accomplished. (Map to agency's technology vision.) GCSS (CINC/JTF) is required to be certified, as a minimum, at DII Common Operating Environment (COE) (DII COE) Level 6?. GCSS (CINC/JTF) V2.0 received a "Joint Interoperability Test Certification" on 30 Nov 01. Subsequent versions will undergo similar interoperability testing required for certification.

Infrastructure Strategy: The program is capitalizing on the current infrastructure in place, using both the DISN and GCCS.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

Hardware requirements are included in funding. DISA/ GCSS (CINC/JTF) is responsible for hardware and software acquisition for server suites located at Hawaii, Korea, Germany, DECC-D Montgomery, and the Pentagon. CINCs and other user Agencies are responsible for client hardware requirements identified for fielding at individual sites. The program also maximizes the use of existing hardware to minimize costs to the user community. If no, by what means is the hardware provided? N/A

GCSS (CINC/JTF) transport requirements are met through infrastructure provided by DISN and Secret IP Router Network (SIRPNET).

GCSS (CINC/JTF) has interdependencies with other acquisitions to include: Global Transportation Network, Joint Total Asset Visibility, Global Status of Readiness and Training System, Joint Operations Planning and Execution System, National Imagery and Mapping Agency and Aeronautical Data Set, Defense Information Systems Network, Global Command and Control System, and Public Key Infrastructure (IA).

Provide justification for custom components. The foundation of the GCSS (CINC/JTF) architecture is COTS technology. Although the program maximizes the use of COTS, custom software is required since COTS products alone cannot meet the mission requirements

Data Architecture is not applicable to GCSS. GCSS (CINC/JTF) does not store any data; it only pulls data from other systems.

The GCSS Family of Systems has an operational architecture as well as an approved Capstone Requirements Document (CRD). Joint Staff/J4 is developing an ORD for GCSS (CINC/JTF). The CRD and ORD are based on the CINC 129 Combat Support Information Requirements.

**F. Security and Privacy:**

Security mechanisms currently being implemented by the Global Combat Support System Commander-in-Chief/Joint Task Force (GCSS (CINC/JTF)) to maintain the confidentiality, integrity, availability and accountability of the hardware/software and data associated with GCSS (CINC/JTF) include: access control utilization via unique access logon ID, individual accountability through the use of DOD PKI, workstation-level access control through DII/COE login mechanism, transaction activity logging via application clients and servers, the use of SSL and VTI to provide two-way authentication and encrypted communication between GCSS clients and servers.

**Privacy assessments are not applicable to GCSS.**

GCSS (CINC/JTF) resides on the SIPRNet; DOD CAC is for NIPRNet applications only, therefore the DOD Common Access Cared is not applicable.

**G. Government Paperwork Elimination Act (GPEA):**  
DOD Strategic GPEA Plan is not applicable to GCSS.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

The program is under DISA Management Oversight (for specifics, see section b, Program Management and Oversight). The program undergoes periodic reviews to ensure the programs are meeting their cost/schedule/performance goals. GCSS is also part of the DISA Performance Contract and reports on progress quarterly.

**A. Original Baseline :**

GCSS has not been rebaselined since initial program establishment

GCSS has not had any milestone slippages since the last president's budget.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

**C. Current Baseline Information:**

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)	120.219	37.851	31.027	31.828	135.613	356.538
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)	102.090	32.557	30.389	31.358	134.265	330.659
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)	(18.129)	(5.294)	(0.638)	(0.470)	(1.348)	(25.879)
Schedule Goals (months)						

- Variances have been less than 10%.
- The changes in funding were due to Executive Decision.
- There has been a less than 10% variance to the budget from last submission
- The CIO/CFO and MDA/IPT would be informed of any variance at Agency Program Reviews with the Vice Director and the Comptroller.

**Actual Performance from Approved Baseline:**

FY2002:

Goal 1: GCSS will undertake development, integration, testing and fielding of capabilities that implement Joint Staff validated, approved, and prioritized functional requirements contained in the GCSS Phase 3 Requirements Identification Document.

Goal 2: Translate requirements from the Phase 3 Requirements Identification Document into technical solutions with cost/schedule/performance parameters in the GCSS Phase 3 Evolutionary Phase Implementation Plan (EPIP) (Field Release 3.x in FY2002). New capabilities include integration of Joint Logistics Advanced Concept Technology Demonstration (JL ACTD) Tools, map-based view on web portal, transportation common operational picture, and additional personnel data.

FY2003:

Goal 1: GCSS will continue to implement and support the DEPSECDEF approved FY02 Performance Goal as stated in the Defense Information Systems Agency's performance contract with updated capabilities based on Joint Staff validated requirements.

Goal 2: Pending DEPSECDEF approval, GCSS will undertake development, integration, testing and fielding of new capabilities that implement Joint Staff validated, approved, and prioritized functional requirements defined through the Rapid Improvement Team (RIT) Pilot Process, as designated by the DOD CIO & USD AT&L. New capabilities include improved infrastructure, additional data sources (as they become available), and additional requirements as defined by Joint Staff/J4

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

The measurable performance benefits or goals for this segment or phase of this initiative are:

FY 2002:

- Continue fielding GCSS (CINC/JTF) V2.0 to EUCOM and Components, NMCC, USFK and SOUTHCOM.
- Complete integration and testing of the Common Operational Picture - Transportation Support Enhanced (COP TSE).
- Conduct an operational and security assessment of GCSS (CINC/JTF) V3.0
- Begin fielding GCSS (CINC/JTF) V3.0 to locations as prioritized by the Joint Staff
- Integrate JL ACTD capabilities, to include: Force Browser, Sustainment Visibility Tool and Capability Assessment Tool
- Incorporate new functionality, to include: Personnel, medical asset, all mode transportation visibility; Ground track/unit enhancements; Dynamic web-based map visualization
- Provide system upgrades and rapid fixes such as Information Assurance Vulnerability Alert (IAVA) patches to the CINCs in support of current operations Noble Eagle and Operation Enduring Freedom
- Continue to operate and sustain the currently fielded system
- Provide Helpdesk, problem resolution support, remote system administration to the users
- Support exercises, such as Bright Star and Millennium Challenge as well as demonstrations as prioritized by the Joint Staff
- Refresh and maintain hardware/software

FY2003:

- Continue fielding GCSS (CINC/JTF) V3.0 to sites as prioritized by the Joint Staff
- Begin integration of Joint Theatre Logistics (JTL) ACTD capabilities
- Begin integration of Information Dissemination Management (IDM) Capabilities
- Provide access to medical data
- Update training for users and administrators
- Provide system upgrades and rapid fixes such as IAVA patches to the CINCs in support of current operations.
- Continue to operate and sustain the currently fielded system
- Provide Helpdesk, problem resolution support, remote system administration to the users
- Support exercises, and demonstrations as prioritized by the Joint Staff
- Refresh and maintain hardware/software

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DOD Component: Defense Information Systems Agency (DISA)

FY 2004-08

- Continue to operate and sustain the currently fielded system
- Complete integration and fielding of the collaborative planning tools for the JTL (Joint Theatre Logistics) ACTD
- Upgrade all systems and applications software to latest technology
- Incorporate wireless data entry and distribution mechanisms into GCSS architecture
- Integrate and deliver coalition tools from the Coalition Theater Logistics (CTL) ACTDs which pass military assessment
- Incorporate new data sources as directed by the Joint Staff to satisfy evolving CINC requirements
- Continue to provide system upgrades and security enhancements such as IAVA patches in support of current operations
- Continue to support exercises and demonstrations as prioritized by the Joint Staff
- Continue to refresh one third of hardware and software each year

**Cost and Schedule Corrective actions:** There have been no corrective actions necessary on the GCSS Program.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: Defense Information Systems Network – Long Haul (DISN-LH).  
Budget Initiative Number: 0595

IT Registration System Number ALDISA03 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: Mission Critical

Information Technology Project or National Security System: Information Technology Project

Program Activity/Mission Area: Communications & Computing Infrastructure (C&CI) – B.2. Communications Infrastructure

### PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was Initiated: 11 September 1991

Projected Date for Completion of Phase; on-going and of Project Ongoing.

Acquired components of the DISN Program are viewed by the DISA Procurement Executive.

Date of Last Acquisition Decision Memorandum (ADM): The date of the last Acquisition Decision Memorandum (ADM) was in 1994 for DISN CONUS.

Project is in N/A PHASE or MILESTONE, Approval Dated: N/A,        Phase as of current review.

The DISN program is reviewed in the Major Automated Information System (MAIS) Report on a quarterly basis.

No programmatic weaknesses have been identified. Major directed changes are in the process of being incorporated into the GIG expansion.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**  
**Information Assurance.**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?  
Yes ☒ No ☐
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 0 The Agency maintains a separate IA Program in support of all major Agency IT Initiatives.
3. Has DoD or Component CIO reviewed this project for CCA Compliance? Yes ☒ No ☐

Clinger-Cohen Compliance is documented and reviewed under the Annual Program Plan Review and the Quarterly In-Process Reviews, which the DISA CIO is a part of. The most recent review of the DISN program was during the FY02 Program Plan Review held 30 August 2001. DISN was considered compliant with the Clinger-Cohen Act.

4. Does this initiative implement electronic transactions or record keeping?  
▪ Was a privacy impact assessment performed on this project?  
Yes ☐ No ☒  
Yes ☐ No ☒

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes.
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review?  
Yes. Changes to the program resources were primarily due to Congressional Adjustments and internal DISA realignments due to the transformation. Were they pricing changes or program changes? Yes. Pricing changes were directed at the Congressional Level.
3. How were the resource costs determined (CAIG, other costing methods, etc)? DISN was selected based upon the recommendations of the OASD (C3I) Data Communications Task Force study report, dated, Aug 1990 and Defense Management Review Decision (DMRD) No. 968. Both addressed the cost benefits of consolidating Department assets into a common-user information transport infrastructure.
4. Federal Financial Managers Improvement Act (FFMIA) is not applicable to the DISN program. The program is not a part of the DOD Financial Management Architectural Improvement Process, nor is this project categorized as a Financial Management or Financial Feeder System.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Part I. B. Summary of Spending for Project Stages:**

Project Name and Acronym: Defense Information Systems Network – Long Haul (DISN-LH)  
Project Activity/Mission Area: Communications, Computing Infrastructure (C&CI) – B.2. Communications Infrastructure.

Component	Dollars in Millions				
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 – FY2007
<b>Planning</b>					
APPN or Fund 1 to n - DevMod	93.978	55.371	16.670	18.595	67.432
Total Dev Mod	93.978	55.371	16.670	18.595	67.432
<b>Full Acquisition</b>					
APPN or Fund 1 to n - Dev Mod	67.523	34.584	33.838	572.203	471.100
Totals Dev Mod	67.523	34.584	33.838	572.203	471.100
<b>Maintenance/ Current Services</b>					
APPN or Fund 1 to n – Current Services	2,725.994	1,364,300	1,701,907	1,600,019	6,629,509
Totals Current Services	2,725.994	1,364,300	1,701,907	1,600,019	6,629,509
<b>Totals Resources by FY</b>	2,887.495	1,454,255	1,752,415	2,190,817	7,168,041
					15,453.023

## Part II: Justification and Other Information

### A. Description:

Defense Information System Network (DISN) provides the warfighters and the Warfighting Commander in Chief (CINCs), Joint Task Force (JTF) Commanders and Combined Task Force (CTF) Commanders with a robust Command, Control, Communications, Computers and Intelligence (C4I) information transport infrastructure. DISN-LH, supports the DOD/Joint Staff/DISA goals associated with C4I for the Warrior, Joint Vision 2010 and Joint Vision 2020, by providing a global, secured interoperable information transport infrastructure in support of the Department's mission and mission needs. It seamlessly spans both the terrestrial and space strategic domains, as well as the tactical domain, to provide the interoperable telecommunications connectivity and value added services required to plan, implement, and support any operational missions anytime and anywhere. DISN provides the warfighters with U.S. Government-controlled and secured voice, data, imagery, video teleconferencing, and dedicated point-to-point transmission services, and enable seamless information transfer processes. With its integrated requirements database, DISN directly supports national defense C4I decision-making requirements, and U.S. efforts to maintain the worldwide lead in defensive information warfare. DISN itself is divided into three blocks composed of the sustaining base (DISN-SB) under the Services and Agencies, the deployed assets (DISN-D) under purview of the Commanders-in-Chief, and the long-haul interconnecting network (DISN-LH) under the purview of DISA. In order to provide a global, secured, interoperable information transport infrastructure in support of the Department's mission and needs, DISA's primary efforts for DISN include: Terrestrial Transmission Services which provides global integrated terrestrial transport platform, operational integration with the satellite communications (SATCOM) infrastructure, and transparent interfaces to Military Department's sustaining base; SATCOM Services which provide space-based transport services with long-haul and deployed terrestrial delivery platform integration; and Global Services, which includes technology assessments, network management, service provisioning services which provide for maintenance and enhancement of network management services/capabilities and network/customer provisioning. The Global Information Grid (GIG) has a planned expansion to be implemented within the global network over the next three years. For historic purposes, schedule milestones are presented for FY01-02 for Information Dissemination Management (IDM) Services, which provide for search/manipulation/dissemination management of information with integrated interfaces to its transport/dissemination platforms, e.g. Global Broadcast System (GBS). Beginning in FY03, the IDM element is moved to a new Program Element, PE 0303149k, and the GBS services will be reported as part of DISN Global Services. Additionally, while remaining a part of the overall DISN, the interface to the CINC's deployed/mobile DISN-D assets, is now addressed under a separate IT Initiative, Teleport, vice this report. All of the above efforts support the DISA/Joint Staff/DOD goals associated with C4I for the Warrior, Joint Vision 2010 and Joint Vision 2020.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DISN-LH, supports the DOD/Joint Staff/ DISA goals associated with C4I for the Warrior, Joint Vision 2010 and Joint Vision 2020, by providing a global, secured interoperable information transport infrastructure in support of the Department's mission and mission needs. DoD Directive 5105.19, delineates the mission of DISA to provide LH common user communications infrastructure.

The pre milestone O/ Planning activities that led up to this decision were the findings of the final report of the OASD (C3I) Data Communications Task Force recommendation, dated, Aug 1991.

DISN was selected based upon the recommendations of the OASD (C3I) Data Communications Task Force study report, dated, Aug 1990 and Defense Management Review Decision (DMRD) No. 968. Both addressed the cost benefits of consolidating Department assets into a common-user information transport infrastructure.

**B. Program Management/Management Oversight:**

COL Timothy J. Fong, USA, Chief, Center for DISN Services  
Ms. Linda Safford, Deputy Chief, DISN Program Manager  
Thomas Thoma, Procuring Contracting Office - DISA/ACQ  
5111 Leesburg Pike, Bailey's Crossroads, VA 22041; Administrative Contracting Office - Defense Information Technology Contracting Office, 2300 East Dr, Scott AFB, IL 66625

DISN uses MAISRC-Member IPT, designated C3I Special Interest Program

Department of Defense  
 Capital Investment Exhibit  
 Fiscal Year (FY) 2003 Budget Estimates  
 Name of DoD Component: Defense Information Systems Agency

**C. Acquisition Strategy:**

DISA awarded the following component contracts of the DISN:

- DISN Switched/Bandwidth Management Services – CONUS (DS/BMS-C), MCI, McLean, VA 22102
- DISN Transmission Services – CONUS/CONUS Enhanced (DTS-C & DTS-CE), AT&T, Washington, DC 20006
- DISN Video Services – Global (DVS-G), AT&T, Washington, DC 20006
- DISN Support Services – Global (DSS-G), SAIC, Vienna, VA 22183
- DISN Global Solutions (DGS), SAIC, Vienna, VA 22183
- DISN Global Solutions (DGS), SETA, McLean, VA 22101-3833'
- DISN Hawaii Information Transport System (HITS), AT&T, Washington, DC 20006
- DISN Gateway MWINS/OPS & Staffing, Motorola, Inc., Scottsdale, AZ 85252-1417
- DISN Transmission Services – Pacific (DTS-P), MCI, McLean, VA 22102
- DISN Managed Transponder Contract (MTC), Lockheed Martin, Clarksburg, MD 20871
- DISN Satellite Transponder Services - Global (DSTS-G), Multiple Awards
  - Artel Inc, Reston, VA 20191
  - Arrowhead Space & Telecommunications Inc, Falls Church, VA 22046
  - Spacelink International LLC, Dulles, VA 20166
- Iridium Airtime, Iridium Satellite LLC, Tempe, AZ 85284
- Iridium GPAP/Maintenance, Iridium Satellite LLC, Tempe, AZ 85284
- Gateway Switch Maintenance, Ericsson, Richardson, TX 75081
- Gateway Switch Maintenance, NexGen, Leesburg, VA 20176

The major portion of contracts are indefinite delivery indefinite quantity (IDIQ) since the Department was unable to specify its requirements in terms of time and/or quantity to allow for selection of another contract type such as fixed price. IDIQ allowed the flexibility to meet those requirements over time and quantities necessary to satisfy the Department's mission. There are fixed price contracts utilized (airtime) where the requirements could be adequately definitized.

None of the contracts would be categorized as "Performance-based." However, the DGS has provisions for performance based task orders.

All contracts, with the exception of the Iridium/Gateway services, were full and open competitions with selecting criteria being contract dependent, being either Best Value or Best Price. The Iridium Satellite LLC, NexGen, Ericsson, and Motorola contracts were awarded via other-than-full-and-open competition with an approved Justification & Authorization.

**D. Alternative Analysis and Risk Management: Describe AoA.**

An analysis was carried out by OASD C3I Data Communications Task Force Study, report dated August 1999, that considered multiple platforms by independent services and agencies vice a single consolidated platform.

An analysis was carried out by OASD C3I Data Communications Task Force Study, report dated August 1999, that considered multiple platforms by independent services and agencies vice a single consolidated platform.

Underlying assumptions. N/A

Estimate of Risks. N/A.

**E. Enterprise Architecture and Infrastructure Standards:**

The DISN infrastructure is the basic common user IT transport system for the DOD. It provides DOD users with a capability that allows the individual system to be interoperable.

The Infrastructure Strategy for DISN is a combination of leased, leased-to-buy, and government-owned equipment and services.

Funding for all DISN long haul hardware requirements are included. One of the primary objectives of the DISN-LH contracts was to provide the vehicles for leased commercial services without the necessity to expend resources for equipment acquisition. The exception is the Iridium Gateway, which acquired system equipment to interface DISN-LH to commercial services.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DISN is the computing and communications transport vehicle, DISN-LH providing the long-haul transport capability.

DISN is interdependent with sustaining base infrastructure (DISN - SB), Service deployed assets (DISN - D), and National Security Agency security initiatives.

DISN uses COTS/Modified COTS Applications

The Data Architecture approach is not applicable.

The functional architecture approach is not applicable.

**F. Security and Privacy:**

DISN Long-haul provides global long haul network backbone transport services, including satellite and terrestrial, to support warfighter missions. All DISN L-H components will be fully certified and accredited IAW the DODI 5200.40, DITSCAP process. Security features, including firewalls, guards and link encryption are employed to safe guard information transmitted across the backbone network. DISN Long-haul provides DOD interoperability and end-to-end integration of automated information systems to improve investment in the DOD information infrastructure. DISN Long-haul component connection approval process is supervised by the joint DOD designated approving authorities and supported by the DISN Security Accreditation Working Group. DISN Long-haul security documentation including, information classification guidance, architecture, policy, and operations procedures, are published to address the defense and protection of information and network systems ensuring their availability, integrity, authentication and confidentiality.

Privacy assessments for the DISN infrastructure are not applicable.

Utilization of the DOD Access Card is not applicable to the DISN infrastructure.

**G. Government Paperwork Elimination Act (GPEA) .**

DISN is not included in the DoD Strategic GPEA Plan. This program, while an IT initiative, provides the IT transport infrastructure only and not the computing infrastructure impacted by the GPEA. DISN provides the electronic transport external to the post, camp, station and base infrastructure.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS.** Incomplete information.

A. The DISN Program was established via Major Budget Issue in FY92 which provided funding in the amount of \$164.7M over six years (FY92-FY97) and provided an additional 145 manpower slots to DISA. Additional changes to this baseline have been directed by multiple Program Budget Decisions. Designated Special Interest item supported by a MAISRC-member IPT. Additional oversight is provided by the Global Information Grid (GIG) General Officers Steering Committee (three-star level), composed of Service and Agencies, Joint Staff and CINC representatives, chaired by ASD(C3I). Resource oversight provided by the DII Resource and Operations Council (three-star level) with representation from Services and Joint Staff currently chaired by DISA Director.

**B. Original Baseline :**

Provide the Analysis of Full Life-Cycle costs (estimates of total cost of ownership.) (Dollars in Millions) and performance benefits or goals for baseline segment or phase of this project. What did you expect to achieve? No Change.

This system has not been rebaselined since initial program establishment.

There has not been any milestone slippages since the last president's budget.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**C. Current Baseline Information:**

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)	2,982.515	1,469.447	1,455.822	1,290.333	7,155.489	14,353.601
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)	2,887.495	1,454,255	1,752,415	2,190,817	7,168,041	15,453,023
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)	0	15.192	296.593	900.484	12.552	1,788.073
Schedule Goals (months)						

There has not been a significant change since the last President's Budget submission.

There has been a change in the FYDP program. The GIG Expansion Program is expected to be funded by OSD with Procurement funds in FY03 and FY04 (\$877M).

**Global Services**

**FY01 – FY02**

**Capstone Documentation (DISN Long-haul Capstones)** - As new technology systems were integrated into DISN, created, updated and maintained the following documentation to support integrated DISN program management and oversight: The Global DISN Program Management Plan, Global DISN Integrated Work Breakdown and Schedule and its migration to the DISN Consolidated Planning Schedule (DCPS), Long-Haul DISN Migration Strategy, and Global DISN Security Plan.

**Capstone Architecture (DISN Long-haul Capstones)** - Updated and maintained the DISN Global Architecture as new systems were integrated into the DISN. Supported the technology convergence studies and design activities associated with DISN and the integration of local, metropolitan, and wide-area networks in accordance with GIG Network Policy.

**Capstone Modeling and Simulation (DISN Long-haul Capstones)** - Provided network design and analysis tools to support the integration and design analysis of the DISN services. On-going studies associated with networking applications with high bandwidth demands impacting network operations. Continued traffic analysis studies and design change recommendations.

**Technology Enhancements Assessments** - Assessed advanced information technologies and COTS products for near-term enhancements to DISN, i.e. Fastlane ATM encryption, Wave Division Multiplexing (WDM) and optical cross-connects, gigabit/terabit routers, MPLS, VPNs, Voice Over IP/ATM, network Information Assurance (I/A), network Quality of Service (QoS). Provided technical leadership in implementing recommended solutions and evolving the DISN. Continue support of DISN/GBS risk reduction trials.

**Network Integration & Waiver Analysis** - Transitioned ISC and other networks onto DISN. Completed transition of SCAMPI terrestrial backbone to DISN. Completed the transition of SCAMPI Network management and O&M to DISN. Initiated work in the Critical Infrastructure Protect domain IAW OSD guidance. Started implementation of the ISO 900 certification process. Supported OSD in the Global Information Grid (GIG) waiver process. Identified and initiated transition of non-DISN services to the DISN. Initiated actions to implement Performance Management and Configuration Management as applicable to the DISN.

**Joint DISN Control System (JDCS)** - Implemented and supported the integration of network management functions for DISN, as well as other DISA pillar programs. Expanded existing JDCS architecture to support the upgrade of the Integrated Network Management System (INMS) to version 3.0 (NeuralStar 6.0); provide backup capability for the DISA Trouble Management System (TMS) and upgrade to Remedy ARS version 4.5.2; migrate the DISA Reports Management System (RMS) from My Eureka to Seagate Info (Crystal Decisions). Produced a standard COE compliant package of the Joint DISN Control System (JDCS) tools. Supported insertion of new technology into the DISA Global and Regional Network Operations and Security Center's architecture and the JDCS. Continued administration, maintenance, and network integration of the INMS at the Global Network Operations and Security Center (GNOSC), which provides the comprehensive status of the GIG.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Joint Defense Information Infrastructure Control System - Deployed (JDIICS -D) (DISN Deployed)** - Fielded 41 JDIICS-D suites and evaluated new COTS/GOTS software products for application to network software tools. Supported the deployed JDIICS-D suites and the transition to the joint network management system under the Army as executive agent. Provided schoolhouse training and developed Computer Based Training for JDIICS-D system users. Provided 24 hour help desk support, configuration management and software development for current and future versions of JDIICS-D.

**Worldwide On-Line System - Replacement (WWOLS-R) (Automated Tools for Service Ordering - ATSO)** - Maintained WWOLS-R while migrating/integrating services from Provisioning 2000 (P2K). Provided full life cycle support for the systems used in provisioning and managing DoD telecommunications assets. Developed, maintained and managed the hardware and software systems of WWOLS-R and Defense Information Systems Network - Integrated. (DISN-I). Services included maintenance of functional applications that support provisioning telecommunications services, adaptation to changing requirements, application and infrastructure stability, Critical Software Maintenance to both the WWOLS-R and DISN-I applications, database administration, and critical hardware maintenance.

**Provisioning 2000 (P2K) (Automated Tools for Service Ordering - ATSO)** - Completed transition of non-DISN data to the IRDB. Developed interfaces and application systems off the PIMS. Maintained and enhanced the P2K systems to support evolving DISA and non-DISA requirements. Integrated Life-Cycle Management support for new DISA services into P2K.

**The Army Distance Learning Program (TADLP) (DISN Global Projects)** - Continued contract support to transition the TADLP to the DISN. Currently provisioned to transition 47 sites with 87 remaining sites. Complete transition is expected by FY-04.

**Air Force Reserve Center System (AFRCS) (DISN Global Projects)** - Begin assisting the Air Force in transitioning their Distributed Learning requirements to the DISN. The Air Force Reserve Center System (AFRCS) consists of 48 sites and 48 rooms to be transitioned by FY04.

**Ground-based Midcourse Missile Defense (GMD)** - Began establishing LH assistance to ASD(C3I), GMD Office, USAF and their support contractors in establishing dedicated LH network capabilities throughout their network architecture. Initial network hub testing conducted in FY02.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Navy/Marine Corp Internet (N/MCI)** - Engineered and installed a Virtual Private Network. WAN Provisioning Process Document (CONOPS), NMCI architectural design, program management plan, and business case were developed to satisfy Navy urgent requirements. Developed NMCI Security Policy, Security Architecture, Configuration Plan, and Risk Management Plan.

The Communications DWCF supports the day to day business operations of the DISN. The DISN strategy is to consolidate the Military Departments' and Defense Agencies' telecommunications networks into one common-user network with interoperable equipment. DISN services are grouped into seven lines of business:

1. Transmission Services
2. Data Services
3. Voice Services
4. Video Services
5. Messaging Services
6. Tier One
7. Reimbursable Communications Services

A description of each Service follows:

**Transmission** - Provides a robust world wide capability of day to day voice, video, data and message transmission for the Service Components and Defense Agencies. Transmission continues to increase infrastructure to accommodate growth in demand. Also, DISA continues the installation of the OCONUS transmission system as well as expanding the Continental transmission system. .

**Data** - Accommodate continuing demands in growth through the migration of legacy service networks to Data. Continue the transition to Gigabyte Routers from Internet Protocol Routers in order to increase network capabilities as well as serve Community of Interest (COINS) customers. Data provides secure internet protocol (SIPRNET) as well as non-classified internet protocol (NIPRNET) capabilities. In order to more accurately associate cost of operations to benefiting customer Data is working to implement usage based billing.

**Voice** - Includes the operation of the Defense Switched Network (DSN), Hawaii Information Transfer System (HITS), Enhanced Mobile Satellite System (EMSS), Defense Red Switch Network (DRSN). Voice provides day to day commercially competitive services, unique secure

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Military unique requirements, while charging competitive rates. Voice continues the implementation of day to day operational capabilities in EMSS as well as meeting the demands for increased DRSN installations.

Video – Provides both routine and classified day to day video teleconference capabilities for the Department of Defense. Video has experienced a surge in demand for worldwide secure teleconferences. Further, the increased demand for video teleconferencing has resulted in the installation of a COTS time reservation system. The current DVS-G contract expires in April 2003. Video is evaluating alternative successor contract possibilities.

Messaging – Provides day to day organizational messaging for the DOD. The network provides Top Secret, Secret and Unclassified messaging capabilities using four regional Security Operations Centers (DMS Transition Hubs). Messaging is in the process of evaluating the possibility of migrating to a single national Operations Center.

Tier-One pricing recovers the costs of the core infrastructure required to produce military readiness attributes of the DISN. In FY 2002 Tier-One funds were transferred to DISA by Congressional direction from the customer. In FY 2003, DISA returns to the procedure of recovering Tier-One cost through a monthly recurring charge to the Service/Agency component levels.

Reimbursable - In addition to the DISN, Telecommunication Services provides a wide variety of cost-reimbursable services for the Department of Defense Community and other organizations. This mainly includes unique reimbursable point-to-point telecommunication service contracts, and FTS 2000 and FTS 2001 service.

**FY03**

**Capstone Documentation (DISN Long-haul Capstones)** - Update and maintain DISN documentation as new technology systems are integrated into DISN.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Capstone Architecture (DISN Long-haul Capstones)** - Perform studies to support the incorporation of next generation technologies into the DISN. Determine and refine the strategic, operational, system, and technical architectures for the various DISN services and integrate them in an effort to gain synergy between the system infrastructures.

**Capstone Modeling and Simulation (DISN Long-haul Capstones)** - Continue network design and analysis tools support to the integration and design analysis of DISN services. Continue on-going studies associated with networking applications with high bandwidth demands impacting network operations. Continue traffic analysis studies and design change recommendations.

**Technology Enhancements Assessments (Intelligent Network)** - Assess information technologies and COTS products for near-term enhancements to DISN and provide technical leadership in implementing recommended solutions. Continue to provide technical guidance in evolving the DISN.

**Network Integration & Waiver Analysis** - Continue Critical Infrastructure Protect domain work per direction of OSD guidance. Gain ISO 900 certification. Support OSD in the Global Information Grid (GIG) waiver process. Continue to identify and initiate transition of non-DISN services to the DISN. Begin implementation of Performance Management and Configuration Management for the DISN.

**Joint DISN Control System (JDCS)** - continue the integration of DISN networks into the Integrated Network Management System (INMS); produce a standard COE compliant package of the Joint DISN Control System tools. Support insertion of new technology into the DISA Global and Regional Network Operation and Security Center's (GNOSC, RNOSC) architecture. Continue administration, maintenance, and network integration of the INMS at the GNOSC and RNOSC, which provides the comprehensive status of the DISN.

**Joint Defense Information Infrastructure Control System - Deployed (JDIICS-D) (DISN Deployed)** - Continue the evaluation and integration of JDIICS-D management and control software tools into the Joint Network Management System (JNMS). Assist Army in preparing the objective JNMS. Maintain and revise when necessary the JDIICS-D user, training and implementation guides. Develop follow-on versions of JDIICS-D to provide the CINC JTF's current versions of software contained in JDIICS-D and JNMS.

**Global Broadcast System (GBS) (DISN/GBS Integration)** - Continue planning and systems engineering support for integration of GBS into the DII/DISN. Continue DISN connectivity for GBS SBMs.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**World-Wide On-Line System - Replacement (WWOLS-R) (Automated Tools for Service Ordering - ATSO)** - Provide full life cycle support for the systems used in provisioning and managing DoD telecommunications assets. Continue to develop, maintain and manage the hardware and software systems of WWOLS-R and Defense Information Systems Network -- Integrated. (DISN-I). Services include maintenance of functional applications that support provisioning telecommunications services, adaptation to changing requirements, application and infrastructure stability, critical software and hardware maintenance to both the WWOLS-R and DISN-I systems and applications, and database administration.

**Provisioning 2000 (P2K) (Automated Tools for Service Ordering - ATSO)** - Maintain and enhance the P2K systems to support evolving DISA and non-DISA requirements. Integrate Life-Cycle Management support for new DISA services into P2K.

**The Army Distance Learning Program (TADLP) (DISN Global Projects)** - Continued contract support to transition the TADLP to the DISN. Currently provisioned to transition 47 sites with 87 remaining sites. Complete transition is expected by FY-04.

**Air Force Reserve Center System (AFRCS) (DISN Global Projects)** - Continue assistance to the Air Force in transitioning their Distributed Learning requirements to the DISN. The Air Force Reserve Center System (AFRCS) consists of 48 sites and 48 rooms to be transitioned by FY04.

**Ground-based Midcourse Missile Defense (GMD)** - Begin transition of requirements onto dedicated DISN assets to replace interim non-DISN assets.

The Communications DWSF supports the day to day business operations of the DISN. The DISN strategy is to consolidate the Military Departments' and Defense Agencies' telecommunications networks into one common-user network with interoperable equipment. DISN services are grouped into seven lines of business:

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

1. Transmission Services
2. Data Services
3. Voice Services
4. Video Services
5. Messaging Services
6. Tier One
7. Reimbursable Communications Services

A description of each Service follows:

**Transmission** – Provides a robust world wide capability of day to day voice, video, data and message transmission for the Service Components and Defense Agencies. Transmission continues to increase infrastructure to accommodate growth in demand. Also, DISA continues the installation of the OCONUS transmission system as well as expanding the Continental transmission system. .

**Data** – Accommodate continuing demands in growth through the migration of legacy service networks to Data. Continue the transition to Gigabyte Routers from Internet Protocol Routers in order to increase network capabilities as well as serve Community of Interest (COINS) customers. Data provides secure internet protocol (SIPRNET) as well as non-classified internet protocol (NIPRNET) capabilities. In order to more accurately associate cost of operations to benefiting customer Data is working to implement usage based billing.

**Voice** – Includes the operation of the Defense Switched Network (DSN), Hawaii Information Transfer System (HITS), Enhanced Mobile Satellite System (EMSS), Defense Red Switch Network (DRSN). Voice provides day to day commercially competitive services, unique secure Military unique requirements, while charging competitive rates. Voice continues the implementation of day to day operational capabilities in EMSS as well as meeting the demands for increased DRSN installations.

**Video** – Provides both routine and classified day to day video teleconference capabilities for the Department of Defense. Video has experienced a surge in demand for worldwide secure teleconferences. Further, the increased demand for video teleconferencing continues the installation of a COTS time reservation system. The current DVS-G contract expires in April 2003. Video is evaluating alternative successor contract possibilities.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Messaging** – Provides day to day organizational messaging for the DOD. The network provides Top Secret, Secret and Unclassified messaging capabilities using four regional Security Operations Centers (DMS Transition Hubs). Messaging is in the process of evaluating the possibility of migrating to a single national Operations Center.

**Tier-One pricing** recovers the costs of the core infrastructure required to produce military readiness attributes of the DISN. In FY 2002 Tier-One funds were transferred to DISA by Congressional direction from the customer. In FY 2003, DISA returns to the procedure of recovering Tier-One cost through a monthly recurring charge to the Service/Agency component levels.

**Reimbursable** - In addition to the DISN, Telecommunication Services provides a wide variety of cost-reimbursable services for the Department of Defense Community and other organizations. This mainly includes unique reimbursable point-to-point telecommunication service contracts, and FTS 2000 and FTS 2001 service.

**FY04 – FY07**

**Capstone Documentation (DISN Long-Haul Capstones)** - Update and maintain DISN documentation as new technology systems are integrated into DISN.

**Capstone Architecture (DISN Long-haul Capstones)** - Maintain an integrated architecture framework for the DISN and develop a process for architecture development and control. Continue to perform long-range technical forecast and plans for potential adoption into the DISN infrastructure.

**Capstone Modeling and Simulation (DISN Long-haul Capstones)** - Provide network design and analysis tools to support the integration and design analysis of the DISN services. Continue on-going studies associated with networking applications with high bandwidth demands impacting network operations. Continue traffic analysis studies and design change recommendations.

**Technology Enhancements Assessments (Intelligent Network)** - Assess information technologies and COTS products for near-term enhancements to DISN and provide technical leadership in implementing recommended solutions. Continue to provide technical guidance in evolving DISN.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Network Integration & Waiver Analysis** - Continue work in the Critical Infrastructure Protect domain IAW OSD guidance. Retain ISO 900 certification. Continue support to OSD in the Global Information Grid (GIG) waiver process. Continue transition of non-DISN services to the DISN. Continue implementation and refinement of Performance Management and Configuration Management for the DISN.

**Joint DISN Control System** - Implement and support the integration of network management functions for DISN, as well as other DISA pillar programs. Migrate integrated network management applications to DII COE compliance; produce a standard COE compliant package of the Joint DISN Control System tools. Support insertion of new technology into the DISA Global and Regional Network Operation and Security Center's (GNOSC, RNOSC) architecture. Continue administration, maintenance, and network integration of the Integrated Network Management System (INMS) at the GNOSC and RNOSC, which provides the comprehensive status of the DISN.

**Joint Defense Information Infrastructure Control System- Deployed (JDIICS-D) (DISN Deployed)** - Continue the evaluation and integration of JDIICS-D management and control software tools into the JNMS. Support Army fielding of objective JNMS. Continue necessary the JDIICS-D user, training and implementation guides. Provide integration oversight for the JNMS for deployed forces. Develop follow-on releases of JDIICS-D, as necessary, to provide the CINC JTF systems current.

**Global Broadcast System (GBS) (DISN/GBS Integration)** - Continue planning and systems engineering support for integration of GBS into the DII/DISN. Continue DISN connectivity for GBS SBMs.

**Worldwide On-Line System - Replacement (WWOLS-R) (Automated Tools for Service Ordering - ATSO)** - Provide full life cycle support for the systems used in provisioning and managing DoD telecommunications assets. Continue to develop, maintain and manage the hardware and software systems of WWOLS-R and DISN-I.

**Provisioning 2000 (P2K) (Automated Tools for Service Ordering - ATSO)** - Maintain and enhance the P2K systems to support evolving DISA and non-DISA requirements. Integrate Life-Cycle Management support for new DISA services into P2K.

**The Army Distance Learning Program (TADLP) (DISN Global Projects)** - Complete transition of TADLP Distributed Learning requirements to the DISN. Continue to work with Army in fulfilling future expansions of DL capabilities to the warfighters. Continued contract support to transition the remainder of TADLP to the DISN.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Air Force Reserve Center System (AFRCS) (DISN Global Projects)** - Complete transition of current Air Force Distributed Learning requirements to the DISN. Continue to work with Air Force in satisfy future Distributed Learning communications/distribution needs.

**Ground-based Midcourse Missile Defense (GMD)** - Maintain DISN-LH support to core GMD network-wide requirements.

The Communications DWCF supports the day to day business operations of the DISN. The DISN strategy is to consolidate the Military Departments' and Defense Agencies' telecommunications networks into one common-user network with interoperable equipment. DISN services are grouped into seven lines of business:

1. Transmission Services
2. Data Services
3. Voice Services
4. Video Services
5. Messaging Services
6. Tier I
7. Reimbursable Communications Services

A description of each Service follows:

**Transmission** - Provides a robust world wide capability of day to day voice, video, data and message transmission for the Service Components and Defense Agencies. Transmission continues to increase infrastructure to accommodate growth in demand. Also, DISA continues the installation of the OCONUS transmission system as well as expanding the Continental transmission system. .

**Data** - Accommodate continuing demands in growth through the migration of legacy service networks to Data. Continue the transition to Gigabyte Routers from Internet Protocol Routers in order to increase network capabilities as well as serve Community of Interest (COINS) customers. Data provides secure internet protocol (SIPRNET) as well as non-classified internet protocol (NIPRNET) capabilities. In order to more accurately associate cost of operations to benefiting customer Data is working to implement usage based billing.

**Voice** - Includes the operation of the Defense Switched Network (DSN), Hawaii Information Transfer System (HITS), Enhanced Mobile Satellite System (EMSS), Defense Red Switch Network (DRSN). Voice provides day to day commercially competitive services, unique secure

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Military unique requirements, while charging competitive rates. Voice continues the implementation of day to day operational capabilities in EMSS as well as meeting the demands for increased DRSN installations.

Video — Provides both routine and classified day to day video teleconference capabilities for the Department of Defense. Video has experienced a surge in demand for worldwide secure teleconferences. The current DVS-G contract expires in April 2003. Video is evaluating alternative successor contract possibilities.

Messaging — Provides day to day organizational messaging for the DOD. The network provides Top Secret, Secret and Unclassified messaging capabilities using four regional Security Operations Centers (DMS Transition Hubs). Messaging is in the process of evaluating the possibility of migrating to a single national Operations Center.

Tier-One pricing recovers the costs of the core infrastructure required to produce military readiness attributes of the DISN. In FY 2002 Tier-One funds were transferred to DISA by Congressional direction from the customer. In FY 2003, DISA returns to the procedure of recovering Tier-One cost through a monthly recurring charge to the Service/Agency component levels.

Reimbursable - In addition to the DISN, Telecommunication Services provides a wide variety of cost-reimbursable services for the Department of Defense Community and other organizations. This mainly includes unique reimbursable point-to-point telecommunication service contracts, and FTS 2000 and FTS 2001 service.

#### **Terrestrial Transport Services**

##### **FY01 — FY02**

**Terrestrial Services - Transmission (DISN Global Projects)** - Developed a baseline DISN timing and synchronization architecture. Developed a recommended DISN Timing and Synchron Architecture. Initiated Timing and Synchron architecture upgrade.

**CONUS** — Began and continued modernization and expansion of the infrastructure via the DISN CONUS Expansion initiative to accommodate growth projections in addition to transitioning component's networks that are currently operating outside of the DISN. Implemented Trans-Atlantic ATM. Transitioned DISC and other networks to DISN CONUS and incorporated leading edge technology. Implemented CONUS DISN ATM objective system. Incorporated the Washington Area Wide Band Systems (WAWBS) into the ATM program.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Pacific** - Initiated DTSP contract services: Began DTS-P service cutover and acceptance testing. Transitioned DTS-P contract management to Operations. Monitored DTS-P contractor performance and Engineering Change Proposals (ECPs) recommendations.

**Europe** - Completed industry analysis and network management plan. Continued Defense European Backbone (DEB) and Asynchronous Transfer Mode (ATM) upgrades. Began the DISN-EUR Integrated System Engineering Plan (ISEP). Conducted analysis of extending the DISN-Europe (DISN-E) into CENTCOM & FORCECOM.

**Metropolitan Area Networks** - For NCR Enacted change to program scope. Completed circuit requirements analysis. Conducted market survey analysis. Developed detailed business case to obtain project funding. Released Request for Information and draft Request for Proposal (RFP). Program awaiting development of GIG architecture and strategy. Once funding identified will release RFP.

**Global Secure Communications Network (GSCN)** - Initiated development of a DISN service for HEMP-hardened global survivable communications service supporting nuclear C3 customers and other special users. Began to capitalize on and expand the National Missile Defense (NMD) Communications Network (NCN) efforts to pass to DISA management in FY07. Developed the GSCN Program Management Plan, initial baseline Life Cycle Cost Estimate for the NCN, MOIs with STRATCOM & SIBIRS for requirement development, GSCN CONUS Concept, initial CONUS GSCN system architecture, performance model, ROM cost models, product offering strategy, and cost recovery strategy.

**Terrestrial Services - Switched Circuits (DISN Global Projects) -**

**Defense Switched Network (DSN)** - Operated and maintained the DSN. Completed DSN Program Plan. Prepared Business Case for HITS. Reactivated DSN Configuration Control Board. Submitted request to Joint Staff to redefine DSN Phases II and III to align with current realities and to close out DSN Phase II. Prepared Business Case for the CONUS transition. Completed reevaluation of MLPP rate structure. Completed the Caribbean reconfiguration. Completed updated requirements definition for DSN. Reviewed the DSN Single Systems Management process to consolidate and streamline documentation, update policy and instructions. Completed implementation of ADMISS Configuration Management.

**Defense Red Switched Network (DRSN)** - Provided Agency management support to DRSN, the Special Communications Links (SCL), and the Special Technical Operations group (STO).

**NCA Conferencing Enhancement Program (NCEP)** - Conducted site surveys; developed documentation to support system engineering, testing, concept of operations, and system operations and maintenance training; and conducted installation and testing of Phase I and II.

**European Switch Upgrade** - Initiated and continued European switch upgrades.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Iridium Communications** - Provided continued commercially based voice and low rate data services as a global, secure communications capability in the post-bankruptcy period. Expanded service offering to include low rate data applications in line with commercial offerings. Reviewed/adjusted channel capacity from gateway into DSN based on system growth. FY01 was period of transition to DWCF Reimbursable program per PDB direction.

**Terrestrial Services - Video/Teleconferencing (DISN Global Projects)** - Transitioned DISN Video Teleconference (VTC) services within CONUS and the Pacific to include activation of VTC services to 12 STEP sites. Provided reservation based and dial-up hubbing and interface translation services to the DISN.

**Terrestrial Services - Contracts (DISN Global Projects)** - Conducted industry/government survey of DTS-P service sites. Conducted DTS-P source selection. Awarded DTS-P contract. Initiated planning/execution of DISN CONUS Contract Competitions/Awards including DVS-G, DTS-C, DTS-CE and DGS (DISN Global Services - re-competition of DSS-G and AFNET requirements). Awarded DGS contract. For Code-Division Multiple Access (CDMA) and General Services Mobile (GSM) Wireless Services contract, conducted market research and initiated documentation for system engineering, testing, and system operations, and initiated FAR Part 12 services for CDMA/GSM Wireless phones.

**FY03**

**Terrestrial Services - Transmission (DISN Global Projects)** - Continue Timing and Synchron architecture upgrade.

**Pacific** - Monitor DTS-P contractor performance and evaluate DTS-P annual service technology improvements.

**Europe** - Continue DEB upgrades. Continue analysis of DTS-E and DTS-CENT concept. Finalize DISN-Europe Integrated System Design.

**Metropolitan Area Networks** - For NCR, establish site-specific implementation planning schedule, begins survey and implementation planning, implement and activate service. IOC for Colorado Front Range MAN and NCR MAN. Initiate New Orleans MAN. Continue prevailing technology evaluation and incorporate into the over all GID architecture.

**Global Secure Communications Network (GSCN)** - Continue development of a DISN service for HEMP-hardened global survivable communications service supporting nuclear C3 customers and other special users. Maintain baseline documentation and develop MOIs with other nuclear C3 customers for requirement development. Initiate engineering activities for customers CONUS services.



**Terrestrial Services - Switched Circuits (DISN Global Projects)**

**Defense Switched Network (DSN)** -- Operate and maintain the DSN. Complete/revise DSN-EUR and DSN-PAC network management configuration, basic features, and performance characteristics. Maintain DSN Grade of Service (GOS) and initiate actions to improve GOS where required. Update DSN Circuit Switched Subsystem Interface Criteria. Complete implementation of Common Channel Signaling (CCS) Signaling System 7 (SS7) in the Pacific DSN. Complete the Switched 56/64 KBPS dial up video improvements. Reactivate the DSN Topology working Group.

**Defense Red Switched Network (DRSN)** - Provide Agency management support to DRSN, the Special Communications Links (SCL), and the Special Technical Operations group (STO).

**NCA Conferencing Enhancement Program (NCEP)** - Complete Phase 3 Site testing and implement IOC. Complete program and turn over to MilDeps for O&M.

**European Switch Upgrade** - Initiated and continued European switch upgrades.

**Iridium Communications** - Operate and maintain Iridium Gateway while providing mobile subscriber services of commercially based voice and low-rate data as a global, secure commercial capability. Review/adjust channel capacity from gateway into DSN based on system growth plan for system upgrade. Add additional user features as they become approved and user funded.

**Terrestrial Services - Video/Teleconferencing (DISN Global Projects)** - Provide reservation based and dial-up hubbing and interface translation services to the DISN.

**Terrestrial Services - Contracts (DISN Global Projects)** - Monitor DGS Contract services. For CDMA and GSM Wireless Services, initiate long term contracts for expanded services and customer base, as well as, provide operations and performance management support.

**FY04-07**

**Terrestrial Services - Transmission (DISN Global Projects)** - Continue Timing and Synch architecture upgrade.

**Pacific** - Monitor DTS-P contractor performance and evaluate DTS-P annual service technology improvements.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Metropolitan Area Networks** - FOC for NCR and Colorado Front Range MANs. IOC and FOC of New Orleans MAN. Initiate, IOC and FOC of San Diego, Jacksonville, Norfolk, Pensacola, Puget Sound MANs. Continue prevailing technology evaluation and insertion as feasible

**Global Secure Communications Network (GSCN)** - - Continue development of a DISN service for HEMP-hardened global survivable communications service supporting nuclear C3 customers and other special users. Maintain baseline documentation, MOIs, and requirements documentation. Continue engineering activities for customers CONUS services. Acquire and implement customer connections to the GSCN backbone. Develop GSCN Global Concept and GSCN Global systems architecture. Transition NCN infrastructure to DISN/GSCN. Provision GSCN service to customers.

**Terrestrial Services - Switched Circuits (DISN Global Projects)**

**Defense Switched Network (DSN)** - Operate and maintain the DSN. Complete implementation of Integrated Services Digital Network (ISDN) in the DSN-Pacific. Complete the 51X paths/routing actions. Complete implementation of Common Channel Signaling (CCS) Signaling System 7 (CSS7) in the European DSN. Initiate action for transportable DSN switches. Provide end-to-end view of DSN to Theater CINCs in support of Joint Vision 2020 and the GIG Common Operational Picture. Update DSN Exercise Concept. Complete a CONUS DSN transition. Field transportable DSN switch.

**Defense Red Switched Network (DRSN)** - Provide Agency management support to DRSN, the Special Communications Links (SCL), and the Special Technical Operations group (STO).

**European Switch Upgrade** -- Complete European switch upgrades.

**Iridium Communications** - Operate and maintain Iridium gateway while providing Iridium services of commercially based voice and low-rate data as a global, secure commercial capability. Review/adjust channel capacity from gateway into DSN based on system growth plan for system upgrade and add additional user features as they become approved and user funded.

**Terrestrial Services - Video/Teleconferencing (DISN Global Projects)** - . Provide reservation based and dial-up hubbing and interface translation services to the DISN. Accommodate growth of customer base.

**Terrestrial Services - Contracts (DISN Global Projects)** - Monitor DGS Contract services. Begin work on DTS-P re-compete contract including: Develop Draft SOW/FRS; develop draft program/contract documents; release and analyze results of DTS-P; recompile RFI; develop

**0595/Defense Information System Network (DISN) - IT Capital Investment Exhibit (IT - 300)**

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

initial system design. Finalize DTS-P, recomplete SOW/FRS, programmatic/contracting documents, and system design. Conduct necessary site surveys for recomplete. Release DTS-P Recomplete RFP and evaluate proposals. Award DTS-P recomplete contract. Resolve follow-on technical issues. For CDMA and GSM Wireless Services, continue contracts for services and operations, while supporting expanding user global requirements.

**SATCOM Services**

**FY01 – FY02**

**SATCOM Services -**

**Requirements Support (DISN C4I Requirements and Assessment (ICDB))** - Supported DISN Architecture development and systems integration efforts. Supported Joint Staff J6S in the development of policy and guidance for the use of SATCOM systems. Worked with USSPACE to develop technical and operational assessment procedures for SATCOM payloads. Continued to operate and maintain database and analytic capabilities. Built and configuration managed a software bridge from Joint C4I Decision Support Center (JCDSC) to scenario tool at alternate JCDSC to improve the speed and accuracy of scenario modeling. Investigated the cost of a SIPRNET version of the SATCOM Data Base.

**Architecture (DISN SATCOM Architecture and Integration)** – Completed DISN Strategic Investment Plans, and DISN Decision Roadmaps to guide system acquisition decisions. Conducted mobile user study and reached decision regarding FY2007 need date requirements. Developed Wideband Gapfiller Utilization Concept and Transition Plan, as well as the emerging commercial SATCOM Implementation Plan. Supported SWARF 2000. Provided ongoing support in the development and maintenance of the evolving SATCOM architecture supporting Operation Enduring Freedom. Provided a wide range of architecture assessments and studies in support of the requirements of the Joint Staff, USSPACECOM, NSSA, ASD (C3I) and the services. Complete DepSecDef-mandated Transformational Communications Study.

**SATCOM Services - Operations -**

**Defense Satellite Communications Systems (DSCS)** - Supported pre-launch activities, launch, testing and cutover to operations of DSCS III B-8, B-6 and B-11 satellites. Fielded the windows version of the Interim Tactical Orderwire System. Continued fielding of HT/MT Modernization Program, the bandwidth efficiency modems, and the Universal Modem System. Fielded ATM\SATCOM gateway capability.

**0595/Defense Information System Network (DISN) - IT Capital Investment Exhibit (IT- 300)**  
148

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Enhanced Mobile Satellite Services (EMSS) (DISN EMSS)** - Achieved initial operational capability (IOC) and Full Operational Capability (FOC) of government system. Provided continued commercially-based voice and low-rate data services as a global, secure communications capability through period of corporate bankruptcy. Reviewed/adjusted channel capacity from gateway into DSN based on system growth. FY01 was a period of transition to DWCF Reimbursable Program per PBD 417C direction.

**SATCOM Services - Contracts -**

**International Maritime Satellite Services (INMARSAT)** - INMARSAT services under a replacement contract began global services in FY02 with provisions for DISA management visibility.

**Commercial SATCOM Services** - Continued to offer regional and global access to commercial satellite communications services. Provided satellite communications support for communications networks supporting voice, data, imagery, broadcast and teleconferencing in secure and non-secure modes. Provided SSE support to GSSC and RSSCs.

**DISN Satellite Terminal Services - Global (DSTS-G)** - Awarded contract for 3-year base and 7 one-year options for incremental transponder bandwidth, terminals, and terminal operations. Awarded task orders for transponder bandwidth in direct support of US operations under Operation Enduring Freedom. Monitored contractor performance.

**SATCOM Services - Enhancements -**

**Standard Tactical Entry Project (STEP) (DISN Deployed)** - Augmented EUCOM STEP sites in support of Kosovo air operations. Installed commercial KU SATCOM terminal at Northwest, Virginia STEP site for demonstration and testing of DoD Teleport Program capabilities. Continued planning the fielding of STEP MIDAS equipment. For DISN Deployed Pilot Network, continued integration of advanced technology in the implementation of deployed network and maintained baseline requirements. Provided Kosovo support to EUCOM. Established and operated the DoD Teleport Program Management Office within DISA. Completed the Joint Staff-directed installations of STEP and MIDAS. Monitored operation of STEP sites in coordination with US Army CECOM for improved STEP/MIDAS integration, to include ATM implementation. Continued to incorporate additional technical enhancements to the common equipment baseline. **NOTE: Teleport and STEP/MIDAS activities have been moved into a new PE (0303610K) and will be contained in a separate exhibit for FY02 and out.**

**Enhanced Mobile Satellite Services (EMSS) (DISN EMSS)** - Completed development and certification of the secure user terminal. Completed fixed gateway security firewall integration. Obtained Secure Compartmented Information Facility (SCIF) certification of the

**0595/Defense Information System Network (DISN) - IT Capital Investment Exhibit (IT- 300)**

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

gateway. Completed testing of Type 1 security module for secure user terminal. Expanded service offering to include low-rate data applications in line with commercial offerings. Project transitioned to Iridium Communications.

**DSCS** - Supported next generation Gapfiller SHF satellite acquisition and developed user service requirements and system specifications. Started the Interim Tactical Orderwire System (ITOS) integration into DSCSOC's and effected transfer of ITOS item manager responsibility to Army. Initiated acquisition of AN/GSC-52 Modernization program and CNPS. Acquired ATM\SATCOM gateway capability.

**FY03**

**SATCOM Services -**

**Requirements Support (DISN C4I Requirements and Assessment (ICDB))** - Continue to operate and maintain database and analytic capabilities. Continue to support DISN SATCOM architecture development and system integration efforts. Continue to support Joint Staff J6 and USSPACECOM.

**Architecture (DISN SATCOM Architecture and Integration)** - Develop Wideband Gapfiller Management Plan. Finalize POM 04 Decisions (SWARF 02). Implement Partnerships with commercial service providers. For the NCA Voice Conferencing, complete documentation and begin Phase III installations and testing. Continue to provide support to the Operation Enduring Freedom SATCOM architecture as it evolves. Continue to provide SATCOM architecture products addressing the requirements of the Joint Staff, USSPACECOM, NSSA, ASD (C3I) and the services.

**SATCOM Services - Operations -**

**DSCS** - Field replacement Satellite Command Configuration Element.

**International Maritime Satellite Services (INMARSAT)** - Continue INMARSAT services under DISA management visibility.

**Commercial SATCOM Services** - Continue to offer regional and global access to commercial satellite communications services. Provide satellite communications support for communications networks supporting voice, data, imagery, broadcast and teleconferencing in secure and non-secure modes. Continue leasing transponder capacity in response to requirements for Operation Enduring Freedom. Continue SSE support to GSSC and RSSCs.

**DISN Satellite Terminal Services - Global (DSTS-G)** - Monitor contract and evaluate performance. Evaluate performance for contract option year extensions.

**SATCOM Services - Enhancements** - **NOTE: Teleport and STEP/MIDAS activities have been moved into PE (0303610K) and will be contained in a separate exhibit for FY02 and out.**

**DSCS** - Modernize DSCS terminals for improved throughput, increased logistical supportability and reduced manning.

**FY04 - FY07**

**SATCOM Services -**

**Requirements Support (DISN C4I Requirements and Assessment (ICDB))** - Continue to operate and maintain database and analytic capabilities. Continue to support DISN SATCOM architecture development and system integration efforts. Implement migration plan for integration of SATCOM Control Segment.

**Architecture (DISN SATCOM Architecture and Integration)** - Develop advanced Extremely High Frequency (EHF) CONOPS & Control/Management plan. Finalize advanced WB decision based on 2008 need date. Finalize POM 06 decisions (SWARF 04). Update WB Transition Plan & Teleport Transition Plan. Develop advanced EHF Transition Plan and Mobile User Objective System (MUOS) Transition Plan. For the NCA Voice Conferencing, complete installations and testing and conduct system-wide initial operational test & evaluation.

**SATCOM Services - Operations -**

**DSCS** - Support pre-launch, launch, test and operational cutover of the DSCS III A-3 satellite, as well as first, second and third Gapfiller satellites. Field replacement Defense Satellite Communications System (DSCS) Frequency Division Multiple Access (FDMA) Control System. Field the Common Network Planning Software into DSCS Operations Control System. Complete transition of JRSC to MILSTAR.

**International Maritime Satellite Services (INMARSAT)** - Continue INMARSAT services under DISA management visibility.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Commercial SATCOM Services** - Continue regional and global access to commercial satellite communications services. Provide satellite communications support for communications networks. Provide for a wide range of customer needs supporting voice, data, imagery, broadcast and teleconferencing in secure and non-secure modes.

**DISN Satellite Terminal Services - Global (DSTS-G)** - Monitor contract and evaluate performance. Evaluate performance for contract option year extensions.

**SATCOM Services - Enhancements** - **NOTE: Teleport and STEP/MIDAS activities have been moved into PE (0303610K) and will be contained in a separate exhibit for FY02 and out.**

**DSCS** - Transition Jam Resistant Secure Communications System to MILSTAR. Support the development of the follow-on AWISS satellite system. Modernize DSCS terminals for improved throughput increased logistical supportability and reduced manning. Standardize all control systems to the Objective DSCOC architecture.

**IDM Services** - **Beginning in FY03, the IDM project is moved to a new Program Element, PE, and the GBS services will be reported under DISN Global Services above.**

**FY01 - FY02**

**IDM** - Continued the integration of commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS) and Advanced Concept Technology Demonstration (ACTD) technologies into the IDM software baseline. Three IDM software packages consisting of awareness, access, and delivery core services were developed and released. Government acceptance, DII COE certification, developmental and interoperability tests were conducted. Performed required system engineering, integration, and testing. Provided help desk support. Maintained software licenses. Supported initial fielding and training and later transitioned fielding and training support.

**DISN/GBS Integration** - Continued network and system level integration, performance modeling/analysis, and transmission connectivity planning supporting the fielding of the GBS up-link facilities. Developed and implemented network and system level integration planning to include transmission connectivity engineering and testing (UFO#10). Supported certification testing and accreditation process (UFO#10). Supported full and seamless integration of GBS components and services into the DII/DISN, including Asymmetric Networking and Digital Video. Continued DISN connectivity for GBS Send Broadcast Managers (SBM).

**D. Actual Performance from Approved Baseline:** Summarize what work you planned to accomplish and how much you budgeted to complete the work; What you actually accomplished and how much you actually spent. —

1. Summarize the Performance goals of the acquisition and show how the assess will help the agency meet its overall mission, strategic goals, and annual performance plan. Summarize the in house and contract work goals here. Identify accomplishments to date; describe mission and system performance goals against the milestone schedule, or other schedule. The DISN-Long Haul Measurement Plan Version 1.98 (draft) was prepared to specifically address the need for performance metrics. The Plan outlines the scope and intent of how DISA intends to comply with the Information Technology Management Reform Act (ITMRA) and the Government Performance and Results Act (GPRA). The DISN metrics effort will continue in contract development over the next few years as DISN becomes more robust. Initially, the plan identifies the implementation of four basic categories of metrics: cost, schedule, performance and variance.

Cost measures include period accruals by organization, network, and type of service as well as analytical multi-period trend assessment and forecasting. These cost measures are analogous to the financial reporting found in all large government procurements and commercial programs. In the DISN implementation, cost measures must be developed to cross boundaries of previously "stove-piped" services and new service implementations. Emphasis on analytical assessment and forecasting differentiate these metrics from traditional historic data accrual. Schedule measures include calendar milestone schedules under formal configuration management, milestone achievement status reporting, and milestone achievement assessment and forecasting. These measures combine with cost measures to create historic and expected earned value quantification. Performance measures include network technical performance report accrual, multi-network event comparison, network event repeatability assessment and forecasting, and customer satisfaction measures. Combined with cost and schedule measures, performance measures allow PMO assessment and projection of mission achievement. DISN technical performance measures are to be machine-generated and stored in a central data repository as part of the DISN transition implementation, while customer satisfaction measures are less finite and more subjective in their capture. Variation measures, including assembled common cost, schedule and performance measures of actual DISN performance against plan allow multiple common characteristic identification and assessment for use in the PMO management tool set. Using measurements accrued for technical purposes during the normal function of DISN services, variance forecasts base on multiple parameters, leading indicators and trend evaluation provide mission assurance for the warfighter. Customer satisfaction trend measures are required to assure continuing mission assurance.

Enterprise-level assembly of cost, schedule, performance and variance measures allow combination of data gathered in the course of DISN operation to be applied to assure and to predict success in attaining DISN operating objectives. The metric nature of this assembled data



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

allows quantifiable assessment and prediction with minimum skew from subjective or political pressures while minimizing cost of assembly by maximum use of machine sourced data.

2. Describe the measurable performance benefits or goals for this segment or phase of this initiative.  
FY 2001: **Continued EMSS services through bankruptcy/sale and Digital European Backbone (DEB) & European switch upgrades**  
FY 2002: **Engineer/Install a virtual Private Network to support Navy/Marine Corps Initiatives (NMCI). Continue transition of the Army/AF Distributed Learning Requirements to the DISN.**  
FY 2003: **Begin implementation of diversity of Joint Staff identified sites under the GIG Bandwidth Expansion effort. Expand the Virtual Private Network services the support Army and AF Community of Interest Networks (COINS)**  
FY 2004-07: **Continue to effort to implement the GIG Bandwidth Expansion plus transition all CONUS sites from the current DISN services off the current contracts.**

**Cost and Schedule Corrective actions:** Variance from performance from last submission (identify which submission): Are the performance goals on track since last president's budget submission/last milestone or phase change? **There have been some schedule adjustments in order to maintain the major objectives. Identify any barriers/risks that must be accommodated. Budgetary cuts have caused additional planning/scheduling to maintain the major milestones. Justify variance. Describe corrective actions. Have adjusted some internal schedules that may extend implementation periods (Implementation of Some Distance Learning sites may move out by 3-5 Months).** Include barriers or risks to meeting schedule goals. Describe methods to reduce risk.

1. Identify and discuss corrective actions that have been or will be taken if the current cost or schedule estimates have a negative variance.
2. Identify the effect the actions will have on cost, schedule and performance.
3. Include barriers or risks to meeting funding/cost goals. Describe methods to reduce risk.

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: Common Operating Environment (COE).

Budget Initiative Number: 4018.

IT Registration System Number ALSISA12 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: Mission Critical

Information Technology Project or National Security System: Information Technology Project.

Program Activity/Mission Area: Communications Infrastructure.

### PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was Initiated: 1996

Projected Date for Completion of Project: Ongoing. The COE has no projected end date, as it is an evolutionary program with no specific end. COE is reviewed by the DISA Procurement Executive for your Component.

Date of Last Acquisition Decision Memorandum (ADM): N/A

The COE is not a Major Automated Information System (MAIS). The DISA Vice Director conducts and provides final approval to the COE Annual Program Plan prior to the beginning of the fiscal year. Agency level quarterly Interim Progress Reviews (IPR) are conducted to assess progress and schedule changes.

No weaknesses identified for this initiative in the CIO/program review or during independent evaluations.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

1. The security of this project meets the requirements of the Government Information Security Reform requirements.
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 30%
3. The COE Program is reviewed for CCA Compliance as part of the DISA Annual Program Plan review and through the IT capital planning and investment process via Acquisition Plan documentation. The DISA CIO and the agency Vice Director both participate in this review process.
4. This initiative does not implement electronic transactions or recordkeeping.
5. This initiative was not included in the GPEA strategic plan.
6. No privacy impact assessment was performed on this project.

**RESOURCE REVIEW:**

1. The COE Program received a budget appropriation to support FY002 activities.
2. The COE Program was impacted by applied Congressional financial reductions.
3. Congressional changes directed specific agency product line reductions.
4. The COE Program uses a combination of analogy, actual, and parametric cost methods to determine resource requirements.
5. Federal Financial Managers Improvement Act (FFMIA)
  - COE is part of the DoD Financial Management Architectural Improvement Process.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Defense Information Systems Agency

- COE is not categorized a Financial management or Financial Feeder System.
- FFMIA compliance is not applicable to COE.

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions					
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 - FY 2007	Total
<b>Planning</b>						
APPN or Fund 1to n - DevMod	0					
Total Dev Mod	0					0
<b>Full Acquisition</b>						
APPN or Fund 1 to n - Dev Mod	3.866					
Totals Dev Mod	3.866					3.866
<b>Maintenance/ Current Services</b>						
APPN or Fund 1 to n – Current Services	114.803	32.431	17.415	18.775	87.101	270.525
Totals Current Services	114.803	32.431	17.415	18.775	87.101	270.525
<b>Totals Resources by FY</b>	118.669	32.431	17.415	18.775	87.101	274.391

## **Part II: Justification and Other Information**

### **A. Description/Performance Characteristics:**

The Chairman of the Joint Chiefs has identified as a DOD priority the need for Services and Unified Commands to achieve Automated Information System (AIS) interoperability in Joint Vision 2010. As the infrastructure provider for the Commander in Chiefs (CINC) and Services, DISA established the Common Operating Environment (COE) Program as a means to support this vision. The COE Program provides a DOD infrastructure product that promotes interoperability, portability, and scalability throughout the Defense C2 community. The COE provides a requisite set of core capabilities and establishes, through them, a basis for building interoperable AIS. The COE enables common integrated services sharable by the DOD community in an effective, efficient manner.

The COE provides the ubiquitous foundation for all JTA system architectures to enable operational realization of the Command, Control, Communications, Computers, and Intelligence for the Warrior (C4I<sup>2</sup>W) concept. The COE provides a framework for systems development encompassing systems architecture standards, software reuse, sharable data, secure interoperability, and automated integration. The COE provides new and improved operational capabilities through continuous opportunistic exploitation and integration of commercial-off-the-shelf (COTS) and non-developmental item (NDI) government-off-the-shelf (GOTS) capabilities. The COE prescribes an integration methodology critical to achieving "plug and play" capabilities. The existing COE functional, physical and operational characteristics are consistently upgraded in phased releases. Continued improvements, in accordance with Service and Agency approved requirements and formal build plans, allow mission application developers to target to a specific COE release.

The COE supports the agency mission of planning, developing, fielding, and supporting command, control, communications, and information systems that support the warfighter under all conditions of peace and war. It supports the DISA goal for a flexible, reliable information infrastructure that enables interoperability. The goal of the COE is to provide a distributed application infrastructure that promotes interoperability, portability, and scalability throughout the Global Information Grid (GIG).

The COE Program falls under DISA Business Area 4, the Joint Warfighting and DOD-wide Enterprise Capabilities mission area in the DISA Performance Contract. This mission area is derived directly from the joint warfighter requirements for transmission, messaging, information security, command and control, and combat support as identified in Joint Vision 2010. Of the eight product lines in this mission area, the COE Program falls under Joint Test, Spectrum Management and Engineering. This product line supports joint interoperability testing and certification, spectrum analysis, and common engineering products. The COE Program provides a common, integrated computing environment for use by all DOD application system developers.

The Chairman of the Joint Chiefs, in Joint Vision 2010, established achievement of core capabilities and interoperability needed by all of the Services and Unified Commands within their supporting Automated Information Systems (AIS) as a DOD priority. DISA, as the infrastructure provider for the Commanders-in-Chief (CINCs) and Services, has developed a capability to support the vision in concert with these communities. The COE provides a requisite set of core capabilities and establishes, through them, a basis for building interoperable AIS. The COE is not a system; it is a collection of building blocks (segments), which form the basis for an interoperable system architecture. The COE is the implementation of the system architecture corresponding to the technical architecture defined by the Joint Technical Architecture (JTA). The technical and programmatic effectiveness of this approach has been recognized in the most recent DOD standards. On 22 August 1996, ASD (C3I) approved the DOD Joint Technical Architecture (JTA), Version 1.0. The JTA implementation will permit the quick and seamless flow of information among DOD's sensors, processing and command centers, and shooters to achieve dominant battlefield awareness. The JTA identifies a common set of mandatory information technology standards and guidelines to be used in all new and upgraded C4I acquisitions across DOD. The JTA will be used by anyone involved in the management, development, or acquisition of new or improved C4I systems within DOD. The JTA identifies the concept of a COE that provides a reusable set of common software services via standard application program interfaces (APIs) as the primary mechanism for information processing standards. The use of standard APIs allows the COE and mission applications to be quickly integrated and updated relatively independent of each other. The JTA notes that the COE is the specific implementation that will continue to evolve in compliance with all applicable JTA specifications, standards, and source references. The current JTA Version 3.0, dated 29 November 1999, mandates that all C4I systems shall use the COE. All applications of a system, which must be integrated into the GIG, shall be at least COE Integration and Run-Time Specification (I&RTS) level 5 compliant (software is segmented, uses COE Kernel, and is installed via COE tools) with a goal of achieving level 8.

## **B. Program Management/Management Oversight:**

DISA, as the infrastructure provider for the Commanders-in-Chief (CINCs) and Services, is the executive agent for the COE. A Chief Executive Engineer controls program oversight, guidance, and budget approvals. A COE Project Manager and staff manage the project. The COE Project is not treated as a program but rather a set of services that other systems use to build interoperable capabilities with the DOD. Therefore, the project reports status to the Assistant Secretary of Defense (Command, Control, Communication and Intelligence) (OASD(C3I)) on an as requested basis.

The COE is not a Major Automated Information System (MAIS); however, it follows a consistent Integrated Product and Process Development (IPPD) approach with its use of multidisciplinary Integrated Product Teams (IPTs). This approach allows the project to keep a small government staff while availing itself of the expertise of hundreds of people across the DOD and industry. The Services and Agencies select individuals to work on the sixteen Technical Working Groups (TWGs) which function as IPTs with a designated Chair, agenda, and self-management for scheduling and goal setting. Technical Working Groups generate the Software Requirement Specifications (SRSs) for their technical areas. Technical Working Groups are active in the following functional areas: Administrative Services, Communications Services, Data Access Services (with a sub-group in Database Segmentation), Distributed Computing and Object Management Services, Multimedia/Collaborative Services, Network Management Services, Security Services, Common Operational Picture, Mapping/Charting/Geodesy/and Imagery, Message Processing, Alerts, COE Toolkit, Office Automation, Real-Time, and COE Configuration Management with two subgroups, Enterprise Licensing and Asset Distribution. These IPTs report to a mid-level IPT called an Architecture Oversight Group (AOG) which meets monthly to review TWG processes, assign tasks, and exchange information. The next level IPT is called the AOG Executive Session (AOG-ES) and consists of voting members from the AOG. The AOG-ES meets quarterly and develops a proposed Build Plan. The Build Plan traces to the requirements in the SRSs and recommends when and how a requirement (e.g., a COTS or GOTS product) will be met. The proposed Build Plan is sent to a group which functions as an Overarching IPT, the COE Configuration Review and Control Board (CRCB). The board meets quarterly and consists of flag-level officers from the Services and Agencies who approve the Build Plan and identify resources. In addition to this review thread, every two weeks, COE component contributors attend and update the milestone schedule for the major COE platforms to ensure component development and/or integration is in accordance with the Build Plan schedule and contents. As various components are in process, design reviews are held, open to all interested parties, which address specific design criteria that must be met prior to a component's acceptance into the COE. The COE is an incremental development with major releases every 6 months. This conforms closely to the software release cycle for commercial products. One concept that may be difficult to understand is that the COE is not a system itself; systems are built upon and use COE components and services. The COE does not follow a traditional software development cycle; it is constantly in a requirements freeze, develop, integrate, test, and release cycle for major and minor releases. At any



one point in time, the COE Engineering Office will be working on three releases: the current maintenance release to the user base; the features release planned in 6 month increments to add capabilities to the existing user base, and the next major development release (dependent upon major architecture upgrades).

#### **C. Acquisition Strategy:**

The major contractor for the C2 capabilities within the COE is Northrup Grumman Information Technology (NGIT) 12200 Sunrise Valley Drive Suite 300, Reston, VA 20191. However, the COE is being built currently with task order contracts with eight contractors in addition to NGIT. These contractors will vary during the life of the product set because, as requirements are addressed, different contractors will be best suited to supply the need. The use of multiple contractors garners the capabilities of vendors with the specific skillsets, products and services required to support and intelligently enhance the product set. A wide contractor base also helps diffuse the technology to a broader commercial base, which will, in turn, increase the availability of products for future incorporation into the COE.

The major contractor NGIT, was selected via a sole-source contract because of its in-depth expertise in the development of this type of system. The existing contract is a Cost Plus Award Fee, and quarterly evaluations determine the award fee amounts received. This contract ends in February 03. A competitive acquisition is being worked for a restructured, follow-on contract in FY03 as the COE moves forward to open up its architecture for the next generation of C4I capabilities within the COE to support a more comprehensive common operational picture (COP).

The NGIT contract is not a performance based contract.

#### **D. Alternative Analysis and Risk Management: Describe AoA.**

No formal ROI has been performed for the COE program. Because the COE is not an automated information system, but a collection of infrastructure components used by system developers, the cost savings, cost avoidance, and other benefits from the program are not measured internally. A complete ROI would be identified as a function of the number of COE fieldings throughout the DOD, thereby representing a cost savings or avoidance for each system developer for a set of services provided by the COE. Using this formula, a monetary cost avoidance across the Department could be computed. One reason for the lack of a program ROI is because it is so difficult to get such detailed program cost data from Services and Agencies. The COE provides many other department-wide benefits, including: increased operational and consistent command and control capabilities; increased AIS maintainability and supportability by using COTS hardware and software;



streamlined acquisition techniques using COTS and industry/commercial standards avoiding major duplicative AIS development; AIS life cycle cost savings by providing an open system architecture; AIS systems more flexible for updates, new technologies, and maintenance; Joint Staff validated Command and Control functionality provided across DOD; decrease in DOD training requirements; easier new application integration; and increased DOD interoperability and data access.

No risks have been identified.

#### **E. Enterprise Architecture and Infrastructure Standards:**

The COE itself is a JTA/COE requirement. The JTA mandates that all C4I systems use the COE. All applications of a system, which must be integrated into the GIG, must be at least COE Integration and Run-Time Specification level 5 compliant, with a goal of achieving level 8.

Some hardware is provided as Government Furnished Equipment (GFE) to COE contractors. All GFE is tracked and managed and will be returned to the government upon contract completion. Small amounts of hardware are included for purchasing personal computers and workstations for two small configurations. One configuration is used for test and integration troubleshooting of imminent releases; another is used for evaluating new technologies for future releases. Hardware requirements for both GFE and government configurations are included in this funding.

COE has no interdependencies with other acquisitions.

The COE is characterized by extensive use of COTS except when COTS products are not available for the performance of military niche functions such as support for the Common Operational Picture (COP). The COE consists of kernel services, infrastructure support services, and common support applications necessary to construct a Mission Application. The kernel layer is the minimum set of capability available on any C4I platform. It includes the basic, vendor provided (COTS) operating system with any patches or service packs required to address issues such as security holes, or patches required to support infrastructure services or common support application components. The common desktop for Portable Operating System Interface (POSIX) derivative operating systems is The Open Group (TOG) Common Desktop Environment (CDE) (COTS). COTS RDBMS, Oracle, Sybase, and Informix are used. COTS WWW browsers are used. In all cases, COTS solutions are the first choice.

The COE Service Based Data Architecture provides a strategy for data resource accreditation that allows network components to be independently upgraded without requiring complete "system" rebaselining and re-accreditation. It is a comprehensive strategy that addresses

- Data sharing approaches
- Data storage and access architectures
- Reusable software and data components
- Network service development guidelines & standards and reusable data resources and services, addition/removal of communication paths, update of infrastructure component and addition /removal of applications.

This " Publish and Subscribe" Data Architecture for data services enables a market based data management approach and focuses on services vice platforms or what things can do as opposed to what things are. Services are contractually defined behavior that are provided by any component for use by any component based solely on the contract and are actively managed by the community. This approach eliminates the need for complete "system" rebaselining and re-accreditation when individual components are upgraded, overcomes diversity in languages, middleware, and platforms, encapsulates deployable component, and provides environment where components "plug-and-play."

The COE packages systems components into self-contained units of software called segments. These segments are defined in terms of the functionality provided. These segments can be installed with the tools provided by the COE runtime environment. The COE is a reference implementation of the JTA. It provides common support application and infrastructure services segments to serve as the ubiquitous foundation for all C2 architectures, to enable operational realization of the C4I/TW concept. The COE is not a system, rather it is a foundation for building a shared system.

#### **F. Security and Privacy:**

The security philosophy underlying the DII COE emphasizes, to the maximum extent possible, reliance upon commercial off-the-shelf(COTS) functionality, within the kernel and infrastructure services layer of the COE, for the implementation of security lockdown and features. Several Defense in Depth areas are supported by incorporation of the following features: enhanced kernel and lockdown templates for the protect host computers, enhanced Security Services Architecture Framework (SSAF) for security enabled services, segmented COTS security tool for host monitoring, and enhanced Protect Enclave with SSAF and encryption.

The COE security philosophy is based upon the principle of least privilege: users should be granted access only to those resources required to perform their authorized duties. The COE implements least privilege through identification and authentication of users, discretionary access controls and audit of user activities. This implementation provides a strong technical foundation to ensure users' privacy. Access specific privacy-related data, such as a user's social security number when stored in a database, is the responsibility of the cognizant system's data owner and is beyond the purview of the COE as a system architecture.

The COE SSAF provides the foundation for GOTS application developers to public key-enable (PK-enable) their software consistent with the Department of Defense Public Key Infrastructure (PKI). The current version of SSAF, 1.2, uses software-based certificates while the DoD PKI Program Management Office formalizes its approach to the middleware necessary to access and retrieve users' certificates from a Common Access Card (CAC). The COE Security Engineer consults regularly with the DoD PKI PMO, and a certificate enabled version of SSAF will likely be available in late FY02 or FY03 based upon the availability of CAC middleware.

#### **G. Government Paperwork Elimination Act (GPEA)**

The COE Program promotes the productivity, efficiency, and effectiveness of DoD information technology programs.

### **PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

#### **A. Performance Based Management System (PBMS):**

All contracts deliver monthly status reports on efforts accomplished and planned, deliverables produced, planned and actual schedule/cost/hours expended. All software/main deliverable contributors attend a consolidated bi-monthly schedule meeting for public review and update of schedules. Monthly, and in critical cases, bi-monthly or weekly Progress Status Reviews are held. All deliverables are inspected visually. Software deliverables are inspected visually for completeness and adherence to requirements, directory structure and segment identification requirements, and undergo graphical user interface functional testing and regression testing where applicable. Documentation is reviewed and accepted based on adherence to task order requirements, completeness, and technical merit.

At a macro level, the COE Build Plan is the measure for performance as it covers multiple releases and shows at a glance not only current efforts but past accomplishments or difficulties. It provides an extensive historical record, along with future projections. On a micro level, the Milestone Schedule is a measure for performance for the most imminent release. The Build Plan states the requirement, the computer platforms targeted, the date for accomplishing the requirement, whether or not this requirement will be retrofitted to earlier releases, and the responsible agent. The Milestone Schedule states the requirement, the computer platforms targeted, the date for accomplishing the requirement, and the responsible agent. Documents are color coded with the traditional red (difficulty with performance or schedule), yellow (warning of potential difficulty), blue (in testing), and green (tested and ready for release). Customer acceptance is the greatest performance measurement tool. All COE documentation, to include the Build Plan, is available on the COE homepage for constant review by the entire customer base, in addition to the people involved in the established structure. Customers know what is included in each release. The two performance measures are adherence to schedule and adherence to approved Build Plan contents. Cost as an Independent Variable (CAIV) permeates throughout the structure. When IPTs develop the Source Requirement Specifications (SRS), the Services and Agencies identify their top priorities and these priorities are mapped against available resources. The customer base is realistic and cooperative when trade-offs must be made in performance or schedule. Although formal Earned Value Management (EVM) is not used in the current contract, it is planned for use in the follow-on effort. Many EVM concepts are used, to include: master and intermediate schedules; viewing components as work packages; and paying strict attention to the Budgeted Cost of Work Performed vice the Actual Cost of Work Performed (ACWP), along with an emphasis on schedule.

**B. Original Baseline :**

No formal initial program baseline was established for the COE Program. It is a collection of software components, not an automated system. There is no defined program life-cycle completion date, but rather an evolving baseline of capabilities and technologies that are integrated in a consistent manner that support some 150 DOD programs or systems.

The COE program has revised milestone schedules based on reduced budget in FY02 and the outyears. Schedule goals that were planned, but are now terminated are listed below.

**FY 2002 Schedule Goals Terminated:**

Apr 02 – Deliver COE Release 4.6  
Deliver Kernel Java Installer Specification  
Complete C2PC Functionality (C2PC 5.5.7)  
Begin Web Support Development (Static Web COP)

**FY 2003 Schedule Goals Terminated:**

Oct 02 – Deliver COE Release 4.7  
Deliver Kernel Java Installer Reference Implementation  
Complete Web Support Development (Dynamic Web COP)  
Deliver Componentized ICSF Development Plan  
Deliver Additional C2PC Functionality (as required)

Apr 03 – Deliver COE Release 4.8  
Investigate Real-Time API Patches for Kernel 4.2  
Further C2PC Functionality  
Web Enablement Cleanup  
Deliver Kernel 5.0 Developers Release

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Defense Information Systems Agency

**FY2004/2005/2006/2007 Schedule Goals Terminated:**

Oct 03 – Deliver COE Release 4.9  
Deliver COE Release 5.0  
Deliver Real-Time API Interface to Lynx OS Reference Implementation  
Further C2PC Functionality

Apr 04 – Deliver COE Release 5.1  
Deliver ICSF 5.1

Oct 04 – Deliver COE Release 5.2  
Deliver ICSF 5.2

Apr 05 – Deliver COE Release 5.3  
Deliver ICSF 5.3

Oct 05 – Deliver COE Release 5.4  
Deliver ICSF 5.4

Apr 06 – Deliver COE Release 5.5  
Deliver ICSF 5.5

Oct 06 – Deliver COE Release 6.0  
Deliver ICSF 6.0

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Defense Information Systems Agency

**C. Current Baseline Information:**

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)	118.669	32.431	35.915	37.575	165.601	390.191
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)	118.669	32.431	17.415	18.775	87.701	274.991
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)	0	0	- 48% (18.500)	- 50% (18.800)	- 53% (77.900)	- 70% (115.200)
Schedule Goals (months)						

- Since the last President's Budget submission, Congressional reductions forced cost goal changes greater than 10% in FY02 and outyears.
- Directed Congressional reductions had major impacts on planned program products and capabilities. Specific milestone changes are noted in Section B above.
- DISA applied directed Congressional reductions. The DISA Vice Director and CIO are aware of these cuts, and a revised program plan and program status will be briefed to the Vice Director and CIO at quarterly reviews.



**D. Actual Performance from Approved Baseline:**

The Military Services and Agencies control the COE portfolio. They select and prioritize COTS and GOTS investments based on mission need, risks, benefits, and cost. This prioritization forms the basis of the COE Build Plan and Milestone Schedule. The Build Plan and Milestone Schedule define the requirement, the computer platforms targeted, the date for accomplishing the requirement, whether or not this requirement will be retrofitted to earlier releases, and the responsible agent. The two performance measures are adherence to schedule and adherence to approved Build Plan contents. This approach has proven successful.

Use of the COE promotes achievement of the four operational concepts outlined in Joint Vision 2010 (JV2010): full spectrum dominance: dominant maneuver, precision engagement, full-dimension protection, and focused logistics. These operational concepts are dependent on the ability to collect, process, disseminate, and interpret information to achieve information superiority on the battlefield. The COE is key to information superiority through provision of: a Common Operational Picture for joint and coalition warfare; a method for accelerating dynamic change through application and data reuse; a componentware-based architectural framework supporting secure interoperability, technology insertion, and legacy maintenance; a forum for warfighter agreement on component acquisition and integration; a method for building systems capable of providing focused logistics; and a managed process for continuous integration of advanced technology. The COE is identified as a pivotal technology in the FY2000-2005 Defense Planning Guidance (DPG). As noted in the ASD (C3I) DOD Information Technology Management (ITM) Strategic Plan - Supporting National Defense, V1.0, Mar 97, the COE is an identified model of excellence in meeting the goal of providing services that satisfy customer information needs. The ITM Strategic Plan recommends the COE as a foundation technology for meeting future requirements. The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework, V2.0, Dec 97, notes: "A number of reference models and information standards exist which serve as sources for guidelines and attributes that must be consulted when building architecture products." The COE is listed as a reference model supporting both a system and technical architecture view. The COE provides JV2010 warfighters a significant technical competitive advantage. By building systems utilizing the COE, warfighters can communicate and understand each other, access information needed for focused logistics, interoperate securely, and move toward multi-source correlation of assets and targets which supports dominant maneuver, precision engagement and full-dimension protection and superiority.

Due to reduced funding, COE Program performance goals and milestone schedules have been revised as noted below.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Defense Information Systems Agency

**FY 2002:**

- Goal 1: Deliver Common Operating Environment Release 4.6.
- Goal 2: Provide Maintenance Support for all COE production baselines.

**FY 2003:**

- Goal 1: Provide Maintenance Support for all COE production baselines.
- Goal 2: Deliver incremental enhancements to existing COE baselines by providing customer-directed warfighter improvements needed by DoD application systems.

**FY 2004-07:**

- Goal 1: Provide Maintenance Support for all COE production baselines.
- Goal 2: Deliver incremental enhancements to existing COE baselines by providing customer-directed warfighter improvements needed by DoD application systems.

**Cost and Schedule Corrective actions:**

COE Program milestones and schedules have been adjusted to reflect the reduced funding profile.

Milestone adjustments will allow successful program management within the authorized funding levels.

## PART 1. A. SUMMARY OF PROJECT INFORMATION

### Description Information:

Initiative Name and Acronym: Communications and Computing Infrastructure and Defense Enterprise Computing Centers.

Budget Initiative Number: 5061

IT Registration System Number ALDISA12 (Section 8121, FY 2000 DoD Appropriation)

Mission Critical Status: Mission Critical

Information Technology Project or National Security System: Yes ☒ No ☐  
Program Activity/Mission Area: Communications and Computing Infrastructure

### PROJECT STATUS:

Project Status: New ☐ Ongoing ☒

Date Project was initiated: May 10, 1992

Projected Date for Completion of Phase; \_\_\_ and of Project - Project is on-going.

This project is reviewed by the Procurement Executive for DISA.

Date of Last Acquisition Decision Memorandum (ADM): N/A

Project is in N/A PHASE or MILESTONE, Approval Dated: N/A Phase as of current review.

Budget is reviewed annually and execution is reviewed quarterly by component and OSD.

No weaknesses were identified for this initiative in the CIO/program review or during independent evaluations.

**CLINGER-COHEN ACT COMPLIANCE/CIO REVIEW**

Information Assurance.

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?  
Yes ☒ No ☐
2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 2%  
Yes ☒ No ☐
3. Has DoD or Component CIO reviewed this project for CCA Compliance?  
Yes ☒ No ☐

DISA CIO reviewed the "Acquisition Plan for Consolidated Mainframe and Mid-Tier Proprietary Commercial Off-the-Shelf (COTS) Software Licensing/Maintenance" against the eighteen Clinger-Cohen Compliance questions, defined in the DISA CIO's IT Capital Investment Implementation Plan of December 2000. The AP was found to be fully compliant.

4. Does this initiative implement electronic transactions or recordkeeping? Yes ☐ No ☒

**RESOURCE REVIEW:**

1. Is this project in your baseline resources? Yes
2. Were there changes to your resources (manpower or dollars) during the FY 2002 Amended Budget or during FY 2003 Concurrent Review? Yes. Manpower and labor costs adjusted to reflect actual performance. Pay raise inflation adjusted. There were pricing changes and program changes.
3. Changes to the program were directed at the DoD level.
4. The Defense Enterprise Computing Centers (DECCs) are resourced under the authority of the Defense Working Capital Fund (DWCF). The DWCF provides for business-like operations, whereby the DECCs utilize stabilized rates and full cost recovery to bill for work performed for customers. The DECCs and their detachments negotiate Service Level Agreements (SLAs) with their customers for a defined level of effort, for a particular period (usually a fiscal year). The cost identified in the budget is a consolidation of the cost to support these agreements (stabilized rate and cost reimbursable) with supporting revenue to ensure the DECCs and their detachments are financially viable. Economic analyses are performed for all capital investments.
5. Federal Financial Managers Improvement Act (FFMIA)
  - This project is not a part of the DoD Financial Management Architectural Improvement Process.
  - DECC is not categorized as a Financial management or Financial Feeder System.
  - FFMIA compliance is not applicable to DECC.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 President's Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**Part I. B. Summary of Spending for Project Stages:**

Component	Dollars in Millions				
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 - FY 2007  Total
<b>Planning</b>					
APPN or Fund I to n - DevMod					
Total Dev Mod					
<b>Full Acquisition</b>					
DWCF Capital - Dev Mod*	25.305	23.998	79.030	51.800	201.000
Totals Dev Mod*	25.305	23.998	79.030	51.800	201.000
<b>Maintenance/ Current Services</b>					
DWCF - Current Services*	586.196	586.734	561.586	607.615	2,206.021
Totals Current Services*	586.196	586.734	561.586	607.615	2,206.021
<b>Totals Resources by FY</b>	611.501	610.732	640.616	659.415	2,407.012
					4,929.285

\* FY 2000 only.

## **Part II: Justification and Other Information**

### **A. Description/Performance Characteristics:**

This project description covers the DWCF Computing Services business area of the Defense Information Systems Agency (DISA) and the operations of the Defense Enterprise Computing Centers (DECCs) and their Detachments.

Consistent with Joint Vision (JV) 2020, DISA considers information processing and information technology (IT) to be strategic to achieving information superiority to attain full spectrum dominance. The JV 2020 states, "Information, information processing, and communications networks are at the core of every military activity... The evolution of information technology will increasingly permit us to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. The development of a concept labeled the global information grid will provide the network-centric environment required to achieve this goal. The grid will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel. It will enhance combat power and contribute to the success of noncombat military operations as well." DISA's computing operations are integral components of the global information grid (GIG). To ensure information superiority, these capabilities must be under the military ownership and control that allows them to operate "at a tempo that allows the force to shape the situation or react to changes and accomplish its mission" and to protect against the information operations of an opponent.

The core IT enterprise infrastructure of the GIG resides in the Defense Enterprise Computing Centers (DECCs), previously referred to as Defense Megacenters (DMCs), and their Detachments. The Defense computing infrastructure processes command and control and combat support requirements for warfighters deployed around the world. These requirements include transportation, finance, personnel, munitions, spare parts, medical supplies, and maintenance resources – all critical to military operations. The largest DECC customers are the Army Materiel Command, Air Force Materiel Command, Naval Supply Systems Command, Defense Logistics Agency, and Defense Finance and Accounting Service.

DMRD 918 created DISA's DWCF Computing Services operations in 1992. Since then DISA has had excellent success in continuously reducing the cost of data processing through a series of workload consolidations and technology insertions. The evolution of data centers from dedicated, mission-funded support for their Service or Agency to a DoD multi-service, reimbursable operation within DISA brought about significantly reduced costs and increased interoperability.

DoD accomplished initial data center consolidations with two Defense Management Review Decisions (DMRDs) and the laws incorporating the recommendations of the 1993 Base Closure and Realignment (BRAC) Commission. In an effort to further reduce computing rates and overall costs, and to provide improved service for our customers, DISA developed the Defense Megacenter Business Strategy, signed by the DISA Director on 7 October 1997, and subsequently approved by the Deputy Secretary of Defense. That business strategy showed that by consolidating the mainframe processing from 16 Defense Megacenters (DMCs) to six mainframe processing sites and optimizing operations, DISA could save the Department of Defense \$1.544 billion (FY 1997 dollars) over the 10-year period of the study (FY 1998 - FY 2007). The Strategy for Mainframe and Regional Transition (SMART) plan implemented this strategy beginning in FY 1998. The SMART plan identified 25 specific workload migrations. All but one migration were completed prior to the end of calendar year 1999. The last workload was migrated in August 2000. DISA executed the SMART mainframe consolidation initiative at the same time that customers were fully involved in Y2K preparations. Despite additional requirements and workload migration delays associated with Y2K, DISA was successful in exceeding the expected savings through the end of FY 2001 by 16%.

#### **B. Program Management/Management Oversight:**

The Program Director is DISA's Principle Director for Computing Services (formerly known as WESTHEM), who reports to the Director, DISA. The DISA Director conducts quarterly reviews to evaluate the overall financial health of the DWCF Computing Services business area. The Principle Director for Computing Services conducts more detailed monthly reviews of financial performance at both the site and line of business levels. Designated Computing Services managers conduct individual line of business reviews as needed to discuss strategies and operational concerns. The DISA Director has also established the Defense Computing Business Office to provide analytical, strategic direction and support to the computing services mission, and to establish and manage the computing DWCF POM process within DISA. This submission includes funds for certified audits of financial statements, as required by OUSD(C), starting in FY 2001.



**C. Acquisition Strategy:**

The primary contracting office is the Defense Information Technology Contracting Organization (DITCO). The project uses a variety of competitive Indefinite Delivery/Indefinite Quantity (IDIQ) contracts and GSA Schedules as acquisition vehicles, based on their value to the taxpayer. The initiatives included in this submission are supported by innovative acquisition approaches that provide better responsiveness in addressing processing needs. In order to take advantage of rapidly changing technology and the security and interoperability offered by DISA's facilities, new utility-priced services from the private sector are being used to place current technology on DISA's raised floors simultaneously with demand. "Storage on Demand Services" (SODS) offers timely and flexible disk storage capability at DISA's disposal. Similarly, "Processing on Demand Services" (PODS) offers adaptable CPU services as needed. These capacity-on-demand utilities are proving to be cost effective as well, as we pay only for the capacity we use rather than buying to meet anticipated requirements.

The largest contractual arrangements established by DISA Computing Services are for software maintenance, notably with Unisys Federal Systems, Computer Associates, and International Business Machines.

**D. Alternative Analysis and Risk Management: Describe AoA.**

Between 1990 and 2003, the actions DISA and others have taken to consolidate and optimize mainframe processing will reduce DOD's annual mainframe operating cost from \$1,062 million to \$277 million, a 74 percent decrease. Over the same period, DISA will reduce the number of government civilians supporting mainframe processing by 92 percent, from nearly 10,000 in FY 1990 to 800 projected for FY 2003, and return 984 or 99 percent of all military personnel in DWCF computing operations to the military services. These savings have been realized while MVS/OS390 workload has increased dramatically – by twofold during the same period.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 President's Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

DISA successfully completed phase I of the SMART plan in FY 2000, despite unplanned costs for Y2K, workload migration delays, and increased contract costs, particularly for software, realizing 116 percent of planned savings through the end of FY 2001. With the completion of mainframe consolidation, DISA's attention has shifted to phase II of the SMART plan. SMART Phase II initiatives include DECC Detachment right-sizing, consolidation of overhead functions, mainframe application support services optimizations, and adjustments necessitated by customer workload changes. Although implementation of SMART Phase II will begin in FY 2002, personnel impacts will occur in both FY 2002 and FY 2003. DECC Detachment right-sizing, continued fine-tuning of computing infrastructure, and customer workload changes may necessitate additional personnel adjustments on an annual basis.

During this financial cycle, DISA will establish rates that are fully competitive with commercial service providers, notwithstanding the large variety of executive software demanded by our customers. This will be accomplished by additional optimization and mainframe consolidation to further reduce costs, given that such consolidation must be considered in light of required availability and security, following the events of 11 September 2001.

Information superiority requires continuous availability of IT resources. To that end, DISA is pursuing initiatives, collectively known as "assured computing", that will improve system and data availability to ensure information is continuously available to the warfighter. Implementing the assured computing initiative involves elimination of single points of failure, facility improvements, acquisition of uptime for hardware, and data movement and replication to improve data availability. This process will build upon and improve our existing continuity of operations (COOP) capabilities, and significantly reduce the restoration time to resume operations following a catastrophic failure at any DECC site.

DISA is concluding a rigorous and auditable series of analyses to determine the best architecture for mainframe computing. The result will be a reduction in the number of both MVS/OS390 and UNISYS processing locations that will bring further savings and value to our customers. In order to ensure the best use of resources to improve system and data availability, mainframe consolidation and the assured computing initiative will be integrated into a single implementation plan and occur concurrently. This effort is estimated to require up to \$71 million in investment (capital and operating funds) during FY 2002 and FY 2003, but, once consolidation is completed in FY 2003, will yield annual recurring savings around \$40 million. Approximately half of the savings will result from staffing reductions of at least 300 civilian positions. DISA proposes to apply the positive net operating result from FY 2001 to self-finance this effort.

The 1997 Defense Megacenter Business Strategy was totally successful in defining the glide path for reducing computing costs and improving the quality of computing services. However, the underlying assumptions of the 1997 strategy, especially that of zero workload growth, have now been overcome by events. This submission is based on a replacement business strategy that incorporates further consolidation, assured computing, innovative acquisition strategies, the reality of a changing workload base, and other new initiatives. While this submission is based on further consolidation of mainframe processing locations, that plan must be weighed against the survivability of a more distributed architecture. A robust processing architecture must be maintained to ensure readiness during a sustained campaign against terrorism. We are only beginning to identify the actions and the resources necessary to support such a campaign.

#### **E. Enterprise Architecture and Infrastructure Standards:**

The DECC operations are an integral part of the GIG. The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

**F. Security and Privacy:**

Computing Services exercises defense-in-depth in its approach to security of facilities, networks and systems. The security review program is robust and a multi-layered security architecture is being implemented.

The Computing Services Security Handbook provides guidance to traditional security (physical, personnel, etc.) of DISA's activities. Security Technical Implementation Guides (STIGs) provide specific guidelines for security settings and operations required of operating systems, networks, web applications, and databases. These documents are provided to operating activities as security policy. DISA's central security activity performs onsite and remote annual reviews of operations using the policies as assessment criteria. Security issues are recorded in a security database as findings, and the findings are tracked until they are satisfactorily resolved. Compliance statistics are maintained for each area and are available to commanders and directors at each level. The current compliance level is above 90 percent.

DISA's network security architecture begins with a Joint Intrusion Detection System (JIDS) that passively monitors network traffic at the entries to the local network. The Regional Computer Emergency Response Team (RCERT) at Scott AFB, IL, monitors data from these devices, and suspected intrusive behavior is reported to local Security Managers, as well as the DoD CERT. Premise routers are equipped with filters that deny access to suspected or known sources of intrusive behavior. Local network intrusion detection systems (ISS Realsecure) are employed, and host-based products (currently, AXENT ITA) are utilized to add real-time host intrusion detection capability. Electronic switches are used at facilities to limit entry points and provide for segregation of "community of interest enclaves". Firewall deployments are planned for additional protection and host-based security policy enforcement tools (AXENT ESM on Mid Tier) are also used. A program is in progress to provide audit servers that are designed to protect and consolidate audit records and provide better capability for the review of host generated audit logs. A scanning tool (ISS Internet Scanner) is currently used at least twice a year to remotely examine the network for high-risk vulnerabilities. This IA tool will soon be provided to the local users for adhoc network assessments. Control Centers are protected by a firewall in a separate network segment, as an extra security measure.

DISA has begun to discuss the possible application of the Common Access Card to security in systems, but significant progress in this area may take three to five years.

**G. Government Paperwork Elimination Act (GPEA)**

This project involves the operation and maintenance of a Computer and Communications processing environment rather than management of a functional application.

**PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

The performance measures selected provide an assessment of the areas of performance most critical to DISA Computing Services and its customer as identified during the POM and budget planning periods. DISA Computing Services uses an integrated "Critical Few" Performance Based Management System. The performance measures have been negotiated with DOD and our customers as being critical in supporting customer missions better, faster, and cheaper. The performance measures relate to cost, availability, and quality, with specific measures for this submission shown in section D below. These performance measures are monitored and reported monthly to the Principle Director for Computing Services, and to DISA Headquarters. The DISA Comptroller compiles an annual report for DISA that is submitted to D,PA &E.

The project is reviewed annually prior to actual execution, both at the DISA Headquarters and DUSD(C) levels, through the POM and BES preparation and review cycles. The entire business area is evaluated against the annual budget as a cost evaluation and control process during actual execution. Reviews are conducted monthly with the Principal Director for Computing Services and quarterly at the DISA Headquarters. Appropriate corrective actions, if necessary, are discussed and implemented. Earned value computations are not an appropriate tool for assessing progress in achieving annual or program goals for the ongoing provision of computing services.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 President's Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

**A. Original Baseline:**

The standard acquisition milestones do not apply to this operation because it represents the ongoing provision of services to DoD customers based on their demand. Customer demand and workload changes from year to year and within the actual year of execution. Additionally, actions to improve service or reduce cost are planned and implemented frequently. As a result, the baseline changes at least annually, due to changing workload and cost/performance initiatives.

**C. Current Baseline Information:**

	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)*	\$617.6	\$603.0	\$611.2	\$603.8	\$2,406.9	\$4,842.5
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)*	\$586.2	\$586.7	\$561.6	\$607.6	\$2,206.0	\$4,548.1
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)*	\$(31.4)	\$(16.3)	\$(49.6)	\$3.8	\$(200.9)	\$(294.4)
Schedule Goals (months)						

\* FY 2000 only.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 President's Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

Cost Goals: Cost in this submission is less than in the prior submission in every year with the exception of FY 2003. In no year does the variance from the last submission exceed 10%. FY 2003 is slightly higher due to the requirements of further consolidation of mainframe processing and taking the necessary action to safeguard system and data availability. Outyear costs are lower due to continuation of optimization efforts and further mainframe consolidation. These cost reductions will occur at the same time that assured computing initiatives are implemented and OS/390 and server workloads increase significantly. DISA expects OS/390 workload to increase to a level of 3.7 million CPU hours and UNISYS workload to remain level around 3.3 million SUPs through FY 2003, with further growth in OS/390 to a level of 4.8 million CPU hours and a decline in UNISYS to 1.0 million SUPs through the end of the POM period. General workload growth in OS/390 processing, due to web enabling of applications and other user requirements, will result in increases of 300K – 400K CPU hours annually.

Server-based workload continues to proliferate and the mid-tier platforms themselves are growing larger. Combined with the need to replicate critical real-time data off-site, the overall result is the anticipated revision to the DECC and Detachment architecture, to include consolidation of mainframe and server workload, accompanied by SOE-based pricing mechanisms. Other workload changes are also expected, but not as significant as the growth of server-based workload.

**D. Actual Performance from Approved Baseline:**

Performance goals have been established to reduce cost and improve data availability and processing reliability.

Strategic objective: Significant savings and rate reductions to customers are achieved while providing improved services.

Performance measures:

FY2002

Goal 1: Provide mainframe information processing services while incurring no more than the following unit costs: OS/390 CPU Hour - \$35.76; UNISYS SUP - \$14.67.

Goal 2: DISA will provide at least 98 percent OS/390 and UNISYS platform availability.



Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 President's Budget Estimates  
Name of DoD Component: Defense Information Systems Agency

FY 2003

- Goal 1: Provide mainframe information processing services while incurring no more than the following unit costs: OS/390 CPU Hour - \$28.93; UNISYS SUP - \$13.85.  
Goal 2: DISA will provide at least 98 percent OS/390 and UNISYS platform availability.

**Cost and Schedule Corrective actions:** This submission includes higher levels of customer workload than the previous submission based on direction by D,PA&E to review historical trends over the past several years and DISA's assessment of those trends. One of the benefits of this action is lower stabilized rates for all customers. DISA's performance against the measures above is on target.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: National Communications System

## **PART 1. A. SUMMARY OF PROJECT INFORMATION**

### **Description Information:**

Initiative Name and Acronym: Government Emergency Telecommunications Service (GETS); includes public network priority services for both wireline and wireless priority calls of the National Security and Emergency Preparedness (NS/EP) community.

Budget Initiative Number: 4015

IT Registration System Number:

Mission Critical Status: Mission Critical

Information Technology Project or National Security System: National Security System

Program Activity/Mission Area: Communications and Computing Infrastructure

### **Project Status:**

Project Status: Ongoing

Date Project was Initiated: 1988

Projected Date for Completion of Phase; IOC DEC 2002; Project: Continuing.

Is this project reviewed by the Procurement Executive for your Component?

Yes, the Acquisition Plan was reviewed in accordance with Agency acquisition regulations.

Date of Last Acquisition Decision Memorandum (ADM): Not applicable as this initiative is not a designated Major Automated System or a Major Defense Acquisition Program.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: National Communications System

Project is reviewed in accordance with the thresholds as required in the Agency Acquisition Regulations to include CIO issues. Project performance is regularly reviewed by the inter-Agency GETS User Council. The GETS Program Manager chairs the GETS User's Council to review day-today GETS progress and operations. There have been no major weaknesses identified in this initiative.

**Clinger-Cohen Act Compliance/CIO Review:**

1. Does the security of this project meet the requirements of the Government Information Security Reform requirements?

Not applicable because GETS is not a system but a service for providing priority telecommunications.

2. Percentage of Initiative supporting Information Assurance Activities in FY 2003: 0%

3. Has DoD or Component CIO reviewed this project for CCA Compliance?

Yes, a review was conducted on 28 May 1999.

4. Does this initiative implement electronic transactions or recordkeeping?

No, GETS is a service to provide priority telecommunications, and it is not a system for record keeping and storage

**Resource Review:**

The GETS program and initial work on a Wireless Priority Service were included in the baseline NCS budget. Events of September 11 accelerated the WPS portion of this program responding to homeland security issues. Basic service resource costs are determined from telecommunications company tariffs. New technology efforts are to be costed using independent government cost estimates and will be subject to negotiation as contracts are opened for competition.

The Federal Financial Managers Improvement Act (FFMIA) is not applicable to this system. This system does not process financial information.

**Part I. B. SUMMARY OF SPENDING FOR PROJECT STAGES:\***

Component	Dollars in Millions					
	Cumulative Total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004 - FY 2007	Total
<b>Planning</b>						
APPN or Fund 1 to n - DevMod						
Total Dev Mod						
<b>Full Acquisition</b>						
APPN or Fund 1 to n - Dev Mod						
Totals Dev Mod						
<b>Maintenance/ Current Services</b>						
APPN or Fund 1 to n – Current Services	421.000	22.261	18.190	89.152	109.270	659.873
Totals Current Services	421.000	22.261	18.190	89.152	109.270	659.873
<b>Totals Resources by FY</b>	421.000	22.261	18.190	89.152	109.270	659.873

\*\$101M of Defense Emergency Response Funds (DERF) are not included in above chart

## **Part II: JUSTIFICATION AND OTHER INFORMATION**

### **A. Description/Performance Characteristics:**

The GETS is a service which provides national security and emergency preparedness (NS/EP) telecommunications for the President, Federal, State and local governments, and industry organizations under a broad range of circumstances including natural and man-made disasters. GETS provides NS/EP users a nationwide capability for switched voice and voice-band data communications by exploiting the switching and transmission facilities of the Public Switched Network (PSN), which includes the Local Exchange Carriers (LECs), Inter-Exchange Carriers (IXCs) and wireless carriers. Wireline users have near ubiquitous priority treatment and enhanced routing through the PSN to ensure end-to-end connection under all circumstances of distress or disaster including nuclear attack. Through software changes to the PSN facilities, and use of Personal Identification Numbers (PINs) to authenticate access to these features, GETS ensures that surviving elements of the PSN are available to the NS/EP user community and that priority use of those elements are assured for NS/EP requirements.

### **B. Program Management/Management Oversight:**

The GETS is a project within the OMNCS. The Secretary of Defense is the Executive Agent of the NCS. The OMNCS co-chairs a GETS User's Council to review day-to-day GETS progress and operations.

### **C. Acquisition Strategy:**

The three major long distance carriers (AT&T, Worldcom and Sprint) are used for the transport segment of GETS calls. These long distance carrier contracts were originally awarded in June 1993 as firm-fixed price/sole source contracts. Dyncorp (formally GTE), Chantilly, VA, was selected as the GETS Integration Contractor to acquire local exchange services. This cost plus, award fee (CPAF) contract was originally awarded July 1993. Services from the IXCs have been provided on schedule. These ten year contracts and LECs are currently being modified to meet future service requirements. A Systems Engineering Technical Assistance (SETA) contract was awarded to SAIC originally in 1989 and was extended in 1995. This support is currently being provided under the IAssure contract at DITCO, Scott AFB, IL under a cost plus award fee (CPAF) contract and consists of quality assurance, systems engineering and testing and implementation support. Award fee incentives have been incorporated in GETS contracts where feasible and have proven to be very effective. Performance goals are an inherent

part of PSN services. NS/EP services specify performance as a result of enhanced PSN capabilities and the NCS measures the success of GETS by monitoring call completion rates during periods of extreme network stress to ensure call completion rates are in line with target rates established using models simulating the network at several times overload. An important measure for GETS, and especially for WPS, is speed of implementation. In support of this measure, the NCS established baseline target milestones for implementation and actual switch implementation are measured against the baseline. Competition to acquire services was maximized, however, there is a segment of the acquisition where sole source was employed to ensure redundancy in the long distance (IXC) backbone portion of the PSN. Sole source contracts with the 3 major IXCs fulfill the mandate to utilize the PSN commercially owned assets to the greatest extent possible to implement the most cost effective solution for providing this service. Market research is accomplished through the NCS' daily contacts with industry.

Wireless Priority Service like GETS will involve a broad range of PSN equipment and services; however, new technologies are involved. These include wireless station equipment/handsets, vendor switching capability, transmission capabilities and service support. The WPS acquisition strategy and network upgrades were initiated following the events of September 11, 2001. These upgrades will involve an immediate solution that provided priority access to cellular radio resources in Washington, D.C., New York City, and Salt Lake City also to support the 2002 Olympic Games. A nationwide implementation of end-to-end services is proceeding concurrently and will involve modifications by vendors, carriers and handset providers for end-to-end priority service. Dyncorp in Chantilly, Virginia is serving as the GETS/WPS integrator using the current GETS CPAF contract.

#### **D. Alternative Analysis and Risk Management:**

GETS is a cost effective means of ensuring priority end-to-end connectivity for switched voice and voice-band data communications because it utilizes and leverages the commercially owned assets of the PSN. The Government has realized a tremendous cost savings by utilizing a PSN-based technical approach that takes full advantage of carrier-funded network improvements. In 1992, the White House commissioned a Panel of Experts to conduct an alternatives assessment. The Panel reviewed two approaches for priority service and recommended a PSN-based alternative solution utilizing existing commercially-owned assets in order to leverage future commercially funded network enhancements.

**E. Enterprise Architecture and Infrastructure Standards:**

Because GETS utilizes the standards-based PSN, which employs Signaling System 7 (SS7), it is interoperable with all standard Government telephone networks. GETS is based on the PSN infrastructure and commercially owned assets are utilized. Direct negotiations with switch vendors were conducted and savings were realized for implementing software switch upgrades to support NS/EP calls. These savings accrued through the Government's bulk purchase of commercial items on behalf of all Local Exchange Carriers (LECs).

**F. Security and Privacy:**

GETS cards are issued only to users having a valid NS/EP mission and authentication for user access is accomplished through the use of PINs. Since GETS is PSN-based, it employs industry standard practices of establishing network management operations centers (NMOCs) to monitor indications of potential fraud and to monitor traffic anomalies to detect unauthorized intrusions or network attacks. The combination of PIN authentication and network monitoring secures the services and sets conditions for fraud warnings. Since GETS is PSN-based, it does not employ, nor should it employ, common access card technology. GETS is not a system, it is a service for providing priority service in the PSN to ensure end-to-end connectivity for NS/EP users.

**G. Government Paperwork Elimination Act (GPEA):**

GETS is not a system, but merely a transport mechanism using the PSN for providing for end-to-end priority service to ensure effective communications in an all-hazards environment.



### **PART III: COST, SCHEDULE AND PERFORMANCE GOALS**

#### **A. Management System:**

The OMNCS employs management oversight to monitor adherence to predetermined cost, schedule, and performance targets. Specifically, quarterly reviews are conducted to compare baseline targets to actual achievements. In September 2001, GETS FOC was achieved on time, within budget, and met or exceeded all performance goals (e.g. call completion rates). A similar management review system will be employed to monitor achievement of future goals for the wireless component.

#### **B. Original Baseline :**

Full life cycle costs of \$541M supports operational requirements of NS/EP users with initial local exchange carrier (LEC) and inter-exchange carrier (IXC) enhancements; engineered enhanced routing and priority treatment for the LECs; investigated DISN surge requirements and interoperability; conducted GETS User Council meetings, to include State and local governments; expanded outreach program, to include non-NCS emergency organizations such as the American Red Cross, the Small Business Administration (SBA), the Environmental Protection Agency (EPA), and public utility providers, etc; designed and developed enhanced routing and priority treatment for the LECs and study mobile satellite service interoperability; completed development of enhanced routing and priority treatment for the LECs including first office testing for the LEC switches; began deployment of final LEC enhanced priority treatment features with the LECs; finalized operational support arrangements for the GETS users; reached GETS full-operating capacity. Post GETS FOC requirements will involve operation, administration and maintenance support to ensure efficiency of enhancements to keep pace with the public switched network; and the transition of these capabilities during network convergence of the public switched network.

The service has been rebaselined to implement and manage new technologies, such as the Wireless Priority Service (WPS). The nation-wide phase will implement priority commercial mobile radio system access technology for use end to end throughout the United States, its territories and possessions, using government and industry cooperation and technical experts.

Department of Defense  
Capital Investment Exhibit  
Fiscal Year (FY) 2003 Budget Estimates  
Name of DoD Component: National Communications System

**C. Current Baseline Information: \***

1. What are the cost and schedule goals?	Cum total FY 2000 and prior	FY 2001	FY 2002	FY 2003	Cum Total FY 2004-FY 2007	Total
<b>a. Previous Baseline:</b>						
Cost Goals (\$M)	421.000	21.000	18.190	16.000	65.000	541.190
Schedule Goals (milestones)						
<b>b. Current Estimate:</b>						
Cost Goals (\$M)	421.000	22.261	18.180	89.152	109.270	659.873
Schedule Goals (months)						
<b>c. Variance from Baseline Goals:</b>						
Cost Goals (\$M)	0	1.261	0	73.152	44.270	118.683
Schedule Goals (months)						

\* \$101M of Defense Emergency Response Funds (DERF) are not included in the above chart.

**Cost Goals:**

The GETS wireless component has been accelerated in response to the events surrounding 11 Sep 2001 and in response to White House tasking. As a result of 11 Sep 2001 events, FY01 emergency response funding amounting to \$101M was added to begin development of immediate and nationwide solutions. Funding was added in FY2003 and out-years for the development of a nationwide solution in the current network, and plans to implement into the future generations of technology.

**D. Actual Performance from Approved Baseline:**

Timely implementation was critical for GETS to ensure the service was available to support recovery efforts from natural and man-made events. The events of 11 Sep 2001 showed the need for the same type of capability in wireless networks. In response to White House tasking, the NCS accelerated WPS implementation. In summary, metrics were crafted to support the criticality of speedy implementation. Specifically, baseline schedules were established for switch implementation and actuals were measured against the baseline to ensure implementation targets were met. Implementation of GETS to include WPS supported the mission objective of providing priority service to ensure effective NSEP telecommunications in an all-hazards environment. Effective NS/EP telecommunications are critical to the Nation to respond to and recover from natural and man-made disasters.

**Describe the measurable performance benefits or goals for this segment or phase of this initiative.**

FY 2001: GETS FOC was achieved on schedule to support NS/EP users

FY 2002: Immediate WPS solution was achieved on time to support the Olympics in Salt Lake City

FY 2003: WPS Nationwide IOC will be achieved in FY 2003, as required, to provide a basic architecture and capabilities to NS/EP users

FY 2004-07: WPS Nationwide FOC will be realized and it will be modified to keep pace with technology changes in support NS/EP users

**Cost and Schedule Corrective actions:**

The GETS wireless component has been accelerated in response to the tragic events surrounding 11 Sep 2001 and in response to White House tasking. As a result of 11 Sep 2001 events, FY 2001 emergency response funding amounting to \$101M was added to begin development of immediate and nationwide solutions. Funding was added in FY 2003 and out-years for the development of a nationwide solution in the current network, and plans to implement into the future generations of technology.